ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (EU) 2025/38

z dnia 19 grudnia 2024 r.

w sprawie ustanowienia środków mających na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania cyberzagrożeń i incydentów oraz przygotowywania się i reagowania na takie cyberzagrożenia i incydenty oraz w sprawie zmiany rozporządzenia (UE) 2021/694 (akt w sprawie cybersolidarności)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 173 ust. 3 i art. 322 ust. 1 lit. a),

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Trybunału Obrachunkowego ([1]),

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego ([2]),

uwzględniając opinię Komitetu Regionów ([3]),

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą ([4]),

a także mając na uwadze, co następuje:

(1) Wykorzystanie technologii informacyjno-komunikacyjnych oraz zależność od nich stały się kwestią o zasadniczym znaczeniu we wszystkich sektorach działalności gospodarczej i społeczeństwa w świetle zwiększających się powiązań i współzależności administracji publicznych państw członkowskich, przedsiębiorstw i obywateli w wymiarze międzysektorowym i transgranicznym, a jednocześnie stały się one źródłem potencjalnych podatności.

(2) Na poziomie Unii i na poziomie globalnym rośnie skala, częstotliwość i wpływ incydentów w cyberbezpieczeństwie, w tym ataków na łańcuchy dostaw mające na celu cyberszpiegostwo, instalację oprogramowania szantażującego lub wywołanie zakłóceń. Stanowią one poważne zagrożenie dla funkcjonowania sieci i systemów informatycznych. Z uwagi na szybko zmieniający się krajobraz zagrożeń, zagrożenie możliwymi incydentami w cyberbezpieczeństwie na dużą skalę powodującymi poważne zakłócenie lub uszkodzenie infrastruktury krytycznej wymaga podwyższonej gotowości unijnych ram cyberbezpieczeństwa. To zagrożenie wykracza poza rosyjską wojnę napastniczą przeciwko Ukrainie i prawdopodobnie będzie się utrzymywać, biorąc pod uwagę wielość podmiotów, które mają swój udział w generowaniu obecnych napięć geopolitycznych. Takie incydenty mogą utrudniać świadczenie usług publicznych, ponieważ celem cyberataków są często lokalna, regionalna lub krajowa infrastruktura i usługi publiczne, a władze lokalne są szczególnie podatne na zagrożenia, w tym ze względu na swoje ograniczone zasoby. Incydenty te mogą również utrudniać prowadzenie działalności gospodarczej, w tym w sektorach kluczowych lub innych sektorach krytycznych, powodować znaczne straty finansowe, podważać zaufanie użytkowników, powodować poważne szkody dla gospodarki i systemów demokratycznych Unii, a nawet mieć konsekwencje zagrażające zdrowiu lub życiu. Ponadto incydenty w cyberbezpieczeństwie są nieprzewidywalne, ponieważ często pojawiają się i ewoluują w szybkim tempie, nie są ograniczone do jakiegokolwiek konkretnego obszaru geograficznego i mogą występować jednocześnie lub rozprzestrzeniać się błyskawicznie w wielu państwach. Potrzebna jest zatem ścisła współpraca między sektorem publicznym, sektorem prywatnym, środowiskiem akademickim, społeczeństwem obywatelskim i mediami.

(3) Konieczne jest wzmocnienie konkurencyjnej pozycji przemysłu i usług w całej gospodarce cyfrowej w Unii oraz wsparcie ich transformacji cyfrowej poprzez podniesienie poziomu cyberbezpieczeństwa na jednolitym rynku cyfrowym, jak zalecono w trzech różnych propozycjach Konferencji w sprawie przyszłości Europy. Konieczne jest zwiększenie odporności obywateli, przedsiębiorstw, w tym mikroprzedsiębiorstw, małych i średnich przedsiębiorstw oraz przedsiębiorstw typu start-up, a także podmiotów obsługujących infrastrukturę krytyczną, na rosnące cyberzagrożenia, które mogą mieć niszczące skutki społeczne i gospodarcze. W związku z tym potrzebne są inwestycje w infrastrukturę i usługi oraz budowanie zdolności z myślą o rozwoju umiejętności w dziedzinie

([1]) Opinia z dnia 18 kwietnia 2023 r. (dotychczas nieopublikowana w Dzienniku Urzędowym).
([2]) Dz.U. C 349 z 29.9.2023, s. 167.
([3]) Dz.U. C, C/2024/1049, 9.2.2024, ELI: http://data.europa.eu/eli/C/2024/1049/oj.
([4]) Stanowisko Parlamentu Europejskiego z dnia 24 kwietnia 2024 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z dnia 2 grudnia 2024 r.

cyberbezpieczeństwa, które będą wspierać szybsze wykrywanie cyberzagrożeń i incydentów oraz szybsze reagowanie na nie. Ponadto państwa członkowskie potrzebują pomocy w lepszym przygotowaniu się na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę oraz reagowaniu na nie, a także pomocy w rozpoczynaniu usuwania ich skutków. W oparciu o już istniejące struktury oraz w ścisłej współpracy z nimi, Unia powinna również zwiększyć swoje zdolności w tych obszarach, w szczególności w zakresie zbierania i analizy danych dotyczących cyberzagrożeń i incydentów.

(4) Unia wprowadziła już szereg środków w celu zmniejszenia podatności oraz zwiększenia odporności infrastruktury i podmiotów krytycznych na ryzyka, w szczególności rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 ([5]), dyrektywy Parlamentu Europejskiego i Rady 2013/40/UE ([6]) i (UE) 2022/2555 ([7]) oraz zalecenie Komisji (UE) 2017/1584 ([8]). Ponadto w zaleceniu Rady z dnia 8 grudnia 2022 r. w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej wzywa się państwa członkowskie do wprowadzenia środków oraz do współpracy między sobą, z Komisją i innymi właściwymi organami publicznymi, a także z zainteresowanymi podmiotami, w celu zwiększenia odporności infrastruktury krytycznej wykorzystywanej do świadczenia usług kluczowych na rynku wewnętrznym.

(5) Coraz większe ryzyko w cyberprzestrzeni i ogólnie złożony krajobraz zagrożeń, w tym również wyraźne ryzyko szybkiego rozprzestrzeniania się incydentów z jednego państwa członkowskiego na inne oraz z państwa trzeciego na Unię, wymagają zwiększenia solidarności na poziomie Unii, aby skuteczniej wykrywać cyberzagrożenia i incydenty oraz lepiej przygotować się i reagować na nie, a także skuteczniej usuwać ich skutki, w szczególności poprzez wzmocnienie możliwości istniejących struktur. Ponadto, w konkluzjach Rady z dnia 23 maja 2022 r. w sprawie pozycji UE w kwestiach cyberprzestrzeni wezwano Komisję do przedstawienia wniosku dotyczącego nowego Funduszu Reagowania Cyberkryzysowego.

(6) We wspólnym komunikacie Komisji i Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa z dnia 10 listopada 2022 r. do Parlamentu Europejskiego i Rady zatytułowanym „Polityka UE w zakresie cyberobrony" zapowiedziano inicjatywę na rzecz cybersolidarności UE o następujących celach: wzmocnienie wspólnych unijnych zdolności w zakresie wykrywania, orientacji sytuacyjnej i reagowania dzięki promowaniu wprowadzenia unijnej infrastruktury centrów monitorowania bezpieczeństwa (SOC), wspieranie stopniowego tworzenia na poziomie UE rezerwy do celów cyberbezpieczeństwa, opartej na usługach świadczonych przez zaufanych dostawców, oraz przeprowadzanie testów w krytycznych podmiotach pod kątem potencjalnej podatności na zagrożenia z wykorzystaniem unijnych ocen ryzyka.

(7) Konieczne jest wzmocnienie wykrywania cyberzagrożeń i incydentów oraz orientacji sytuacyjnej w tym zakresie w całej Unii, a także zwiększenie solidarności dzięki zwiększeniu gotowości i zdolności państw członkowskich i Unii do zapobiegania poważnym incydentom w cyberbezpieczeństwie i incydentom w cyberbezpieczeństwie na dużą skalę oraz do reagowania na nie. Dlatego należy ustanowić ogólnoeuropejską sieć centrów cyberbezpieczeństwa (zwaną dalej „europejskim systemem cyberostrzeżeń") w celu zbudowania skoordynowanych zdolności w zakresie wykrywania i orientacji sytuacyjnej oraz wzmocnienia zdolności Unii do wykrywania zagrożeń i udostępniania informacji; należy stworzyć mechanizm cyberkryzysowy, aby wesprzeć państwa członkowskie, na ich wniosek, w przygotowaniu się na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę, w reagowaniu na nie, ograniczaniu ich wpływu oraz w rozpoczynaniu usuwania ich skutków oraz aby wesprzeć innych użytkowników w reagowaniu na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę; należy również ustanowić europejski mechanizm przeglądu incydentów w cyberbezpieczeństwie na potrzeby przeglądu i oceny konkretnych poważnych incydentów w cyberbezpieczeństwie lub incydentów równoważnych incydentom w cyberbezpieczeństwie na dużą skalę. Działania podjęte zgodnie z niniejszym rozporządzeniem powinny być prowadzone z należytym poszanowaniem kompetencji państw członkowskich i powinny uzupełniać, a nie powielać działania prowadzone przez sieć CSIRT, europejską sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe) oraz grupę współpracy (zwaną dalej „grupą współpracy NIS"), ustanowione na podstawie dyrektywy (UE) 2022/2555. Działania te pozostają bez uszczerbku dla art. 107 i 108 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE).

([5]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.U. L 151 z 7.6.2019, s. 15).

([6]) Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (Dz.U. L 218 z 14.8.2013, s. 8).

([7]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.U. L 333 z 27.12.2022, s. 80).

([8]) Zalecenie Komisji (UE) 2017/1584 z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę (Dz.U. L 239 z 19.9.2017, s. 36).

(8) Aby osiągnąć te cele, konieczna jest również zmiana rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/694 ([9]) w niektórych obszarach. W szczególności niniejszym rozporządzeniem należy zmienić rozporządzenie (UE) 2021/694 poprzez dodanie nowych celów operacyjnych związanych z europejskim systemem cyberostrzeżeń i mechanizmem cyberkryzysowym w ramach celu szczegółowego nr 3 programu „Cyfrowa Europa", który obejmuje zagwarantowanie odporności, integralności i wiarygodności jednolitego rynku cyfrowego, zwiększenie zdolności w zakresie monitorowania cyberataków i cyberzagrożeń oraz reagowania na nie, a także wzmocnienie współpracy i koordynacji transgranicznej w dziedzinie cyberbezpieczeństwa. Europejski system cyberostrzeżeń może odegrać ważną rolę we wspieraniu państw członkowskich w przewidywaniu cyberzagrożeń i ochronie przed nimi, a rezerwa cyberbezpieczeństwa UE – we wspieraniu państw członkowskich, instytucji, organów i jednostek organizacyjnych Unii oraz państw trzecich stowarzyszonych z programem „Cyfrowa Europa" w reagowaniu na poważne incydenty w cyberbezpieczeństwie, incydenty w cyberbezpieczeństwie na dużą skalę i incydenty równoważne incydentom w cyberbezpieczeństwie na dużą skalę oraz w łagodzeniu ich skutków. Skutki te mogą obejmować znaczne szkody materialne lub niematerialne oraz poważne zagrożenia i ryzyko dla bezpieczeństwa publicznego. W świetle konkretnych ról, jakie mogą odegrać europejski system cyberostrzeżeń i rezerwa cyberbezpieczeństwa UE, niniejsze rozporządzenie powinno zmienić rozporządzenie (UE) 2021/694 w odniesieniu do udziału podmiotów prawnych z siedzibą w Unii, lecz kontrolowanych z państw trzecich, w przypadku gdy istnieje realne ryzyko, że niezbędne i wystarczające narzędzia, infrastruktura i usługi lub technologia, wiedza fachowa i zdolności nie są dostępne w Unii, a korzyści wynikające z włączenia takich podmiotów przewyższają ryzyko dla bezpieczeństwa. Należy ustanowić szczegółowe warunki, na jakich można przyznawać wsparcie finansowe na działania wdrażające europejski system cyberostrzeżeń i rezerwę cyberbezpieczeństwa UE, oraz ustanawiać mechanizmy zarządzania i koordynacji niezbędne do osiągnięcia zamierzonych celów. Inne zmiany rozporządzenia (UE) 2021/694 powinny obejmować opisy proponowanych działań w ramach nowych celów operacyjnych, a także mierzalne wskaźniki umożliwiające monitorowanie realizacji tych nowych celów operacyjnych.

(9) Aby wzmocnić unijną reakcję na cyberzagrożenia i incydenty, kluczowe znaczenie ma współpraca z organizacjami międzynarodowymi oraz z zaufanymi partnerami międzynarodowymi o podobnych poglądach. W tym kontekście zaufani partnerzy międzynarodowi o podobnych poglądach to kraje, które przestrzegają zasad, które leżą u podstaw Unii, mianowicie zasad demokracji, państwa prawa, powszechności i niepodzielności praw człowieka i podstawowych wolności, poszanowania godności ludzkiej, zasad równości i solidarności oraz przepisów Karty Narodów Zjednoczonych i prawa międzynarodowego, i które nie naruszają podstawowych interesów bezpieczeństwa Unii lub jej państw członkowskich. Taka współpraca może być również korzystna w odniesieniu do działań podjętych zgodnie z niniejszym rozporządzeniem, w szczególności europejskiego systemu cyberostrzeżeń i rezerwy cyberbezpieczeństwa UE. W odniesieniu do europejskiego systemu cyberostrzeżeń i rezerwy cyberbezpieczeństwa UE rozporządzenie (UE) 2021/694 powinno przewidywać, że – z zastrzeżeniem określonych warunków dostępności i bezpieczeństwa – w przetargach dotyczących europejskiego systemu cyberostrzeżeń i rezerwy cyberbezpieczeństwa UE mogą uczestniczyć podmioty prawne kontrolowane z państw trzecich, z zastrzeżeniem wymogów bezpieczeństwa. Podczas oceny ryzyka dla bezpieczeństwa wynikającego z takiego rozszerzenia przetargu należy uwzględnić zasady i wartości, którymi kieruje się Unia i jej partnerzy międzynarodowi o podobnych poglądach, w przypadku gdy te zasady i wartości są związane z podstawowymi interesami bezpieczeństwa Unii. Ponadto w przypadku gdy takie wymogi bezpieczeństwa są rozważane na podstawie rozporządzenia (UE) 2021/694, można wziąć pod uwagę szereg elementów, takich jak struktura korporacyjna i proces decyzyjny podmiotu, bezpieczeństwo danych oraz informacji niejawnych lub szczególnie chronionych, a także zapewnienie, aby wyniki działania nie podlegały kontroli lub ograniczeniom ze strony niekwalifikujących się państw trzecich.

(10) Finansowanie działań na podstawie niniejszego rozporządzenia należy przewidzieć w rozporządzeniu (UE) 2021/694, które powinno pozostać właściwym aktem podstawowym dla działań objętych celem szczegółowym nr 3 programu „Cyfrowa Europa". Szczegółowe warunki uczestnictwa dotyczące każdego działania mają zostać określone w odpowiednich programach prac zgodnie z rozporządzeniem (UE) 2021/694.

(11) Do niniejszego rozporządzenia zastosowanie mają horyzontalne zasady finansowe przyjęte przez Parlament Europejski i Radę na podstawie art. 322 TFUE. Zasady te są ustanowione rozporządzeniem Parlamentu Europejskiego i Rady (UE, Euratom) 2024/2509 ([10]) i określają w szczególności procedurę uchwalania i wykonywania budżetu Unii oraz przewidują kontrole odpowiedzialności podmiotów upoważnionych do działań finansowych.

([9]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/694 z dnia 29 kwietnia 2021 r. ustanawiające program „Cyfrowa Europa" oraz uchylające decyzję (UE) 2015/2240 (Dz.U. L 166 z 11.5.2021, s. 1).

([10]) Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) 2024/2509 z dnia 23 września 2024 r. w sprawie zasad finansowych mających zastosowanie do budżetu ogólnego Unii (Dz.U. L, 2024/2509, 26.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).

Zasady przyjęte na podstawie art. 322 TFUE obejmują również ogólny system warunkowości służący ochronie budżetu Unii ustanowiony rozporządzeniem Parlamentu Europejskiego i Rady (UE, Euratom) 2020/2092 ([11]).

(12) Chociaż środki zapobiegania i gotowości mają zasadnicze znaczenie dla zwiększenia odporności Unii w reagowaniu na poważne incydenty w cyberbezpieczeństwie, incydenty w cyberbezpieczeństwie na dużą skalę i incydenty równoważne incydentom w cyberbezpieczeństwie na dużą skalę, to fakt i czas wystąpienia takich incydentów oraz ich skala są z natury nieprzewidywalne. Zasoby finansowe niezbędne do zapewnienia odpowiedniej reakcji mogą się znacząco różnić z roku na rok i powinno być możliwe udostępnienie ich w trybie natychmiastowym. Pogodzenie zasady przewidywalności budżetowej z koniecznością szybkiego reagowania na nowe potrzeby wymaga dostosowania realizacji finansowej programów prac. Należy zatem zezwolić, aby oprócz przenoszenia środków dozwolonego zgodnie z art. 12 ust. 4 rozporządzenia (UE, Euratom) 2024/2509 możliwe było przenoszenie niewykorzystanych środków, ale tylko na kolejny rok i z wyłącznym przeznaczeniem na rezerwę cyberbezpieczeństwa UE i działania w zakresie wspierania wzajemnej pomocy.

(13) Aby skuteczniej zapobiegać cyberzagrożeniom i incydentom, oceniać je, reagować na nie i usuwać ich skutki, konieczne jest rozwinięcie bardziej kompleksowej wiedzy na temat zagrożeń dla aktywów i infrastruktury krytycznej na terytorium Unii, w tym na temat ich rozmieszczenia geograficznego, wzajemnych połączeń i potencjalnych skutków w przypadku cyberataków mających wpływ na tę infrastrukturę. Proaktywne podejście do identyfikowania i łagodzenia cyberzagrożeń oraz do zapobiegania im obejmuje zwiększenie zaawansowanych zdolności wykrywania. Europejski system cyberostrzeżeń powinien składać się z szeregu interoperacyjnych transgranicznych centrów cyberbezpieczeństwa, z których każde zrzesza co najmniej trzy krajowe centra cyberbezpieczeństwa. Infrastruktura ta powinna służyć krajowym i unijnym interesom i potrzebom w zakresie cyberbezpieczeństwa, wykorzystując najnowocześniejszą technologię zaawansowanego zbierania odpowiednich danych i informacji, w stosownych przypadkach zanonimizowanych, oraz narzędzi analityki, zwiększając skoordynowane zdolności w zakresie wykrywania cyberataków i zarządzania nimi oraz zapewniając orientację sytuacyjną w czasie rzeczywistym. Infrastruktura ta powinna służyć poprawie stanu cyberbezpieczeństwa poprzez lepsze wykrywanie, agregację i analizę danych i informacji w celu zapobiegania cyberzagrożeniom i incydentom, a tym samym uzupełniania i wspierania unijnych podmiotów i sieci odpowiedzialnych za zarządzanie cyberkryzysowe w Unii, w szczególności EU-CyCLONe.

(14) Uczestnictwo państw członkowskich w europejskim systemie cyberostrzeżeń jest dobrowolne. Każde państwo członkowskie powinno wyznaczyć na poziomie krajowym jeden podmiot, którego zadaniem będzie koordynowanie działań w zakresie wykrywania cyberzagrożeń w tym państwie członkowskim. Te krajowe centra cyberbezpieczeństwa powinny pełnić funkcję punktu odniesienia i punktu dostępu na poziomie krajowym do celów uczestnictwa w europejskim systemie cyberostrzeżeń oraz powinny zapewniać, aby informacje dotyczące cyberzagrożeń uzyskiwane od podmiotów publicznych i prywatnych skutecznie i sprawnie udostępniano i gromadzono na poziomie krajowym. Krajowe centra cyberbezpieczeństwa mogą wzmocnić współpracę i udostępnianie informacji między podmiotami publicznymi i prywatnymi, a także wspierać wymianę odpowiednich danych i informacji z odpowiednimi społecznościami sektorowymi i międzysektorowymi, w tym z odpowiednimi branżowymi ośrodkami wymiany i analizy informacji (ISAC). Ścisła i skoordynowana współpraca między podmiotami publicznymi i prywatnymi ma kluczowe znaczenie dla zwiększenia cyberodporności Unii. Taka współpraca jest szczególnie cenna w kontekście udostępniania danych wywiadowczych na temat cyberzagrożeń w celu poprawy aktywnej cyberochrony. W ramach takiej współpracy i udostępniania informacji krajowe centra cyberbezpieczeństwa mogłyby składać wnioski o konkretne informacje i je otrzymywać. Na podstawie niniejszego rozporządzenia krajowe centra cyberbezpieczeństwa nie są zobowiązane ani uprawnione do egzekwowania takich wniosków. W stosownych przypadkach oraz zgodnie z prawem Unii i prawem krajowym informacje, o które wnioskowano lub które otrzymano, mogą obejmować dane telemetryczne, dane z czujników lub dane z rejestrów pochodzące od podmiotów takich jak dostawcy usług zarządzanych w zakresie bezpieczeństwa działających w sektorach kluczowych lub innych sektorach krytycznych w danym państwie członkowskim, aby zwiększyć szybkie wykrywanie potencjalnych cyberzagrożeń i incydentów na wcześniejszym etapie, a tym samym poprawić orientację sytuacyjną. Jeżeli krajowe centrum cyberbezpieczeństwa nie jest właściwym organem wyznaczonym lub ustanowionym przez odpowiednie państwo członkowskie zgodnie z art. 8 ust. 1 dyrektywy (UE) 2022/2555, kluczowe znaczenie ma koordynacja jego działań z właściwym organem w odniesieniu do takich wniosków o udostępnienie takich danych i do ich odbioru.

(15) W ramach europejskiego systemu cyberostrzeżeń należy ustanowić szereg transgranicznych centrów cyberbezpieczeństwa. Te transgraniczne centra cyberbezpieczeństwa powinny zrzeszać krajowe centra cyberbezpieczeństwa z co najmniej trzech państw członkowskich, aby zapewnić pełne osiągnięcie korzyści płynących z transgranicznego wykrywania zagrożeń, udostępniania informacji na ich temat i zarządzania nimi. Ogólnym celem transgranicznych

([11]) Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) 2020/2092 z dnia 16 grudnia 2020 r. w sprawie ogólnego systemu warunkowości służącego ochronie budżetu Unii (Dz.U. L 433 I z 22.12.2020, s. 1, ELI: http://data.europa.eu/eli/reg/2020/2092/oj).

centrów cyberbezpieczeństwa powinno być zwiększanie zdolności w zakresie analizy i wykrywania cyberzagrożeń oraz zapobiegania im, wspieranie generowania wysokiej jakości danych wywiadowczych dotyczących cyberzagrożeń, w szczególności w drodze udostępniania odpowiednich informacji, w stosownych przypadkach zanonimizowanych, w zaufanym i bezpiecznym otoczeniu, pochodzących z różnych źródeł publicznych lub prywatnych, a także przez udostępnianie najnowocześniejszych narzędzi i ich wspólne używanie oraz wspólne rozwijanie zdolności w zakresie wykrywania i analizy tych zagrożeń oraz zapobiegania im w zaufanym i bezpiecznym otoczeniu. Transgraniczne centra cyberbezpieczeństwa powinny zapewnić nowe dodatkowe zdolności, opierając się na istniejących SOC, CSIRT i innych odpowiednich podmiotach, w tym sieci CSIRT, oraz uzupełniając je.

(16) Państwo członkowskie wybrane przez Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa (ECCC) ustanowione rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2021/887 ([12]) w następstwie zaproszenia do wyrażenia zainteresowania w celu ustanowienia krajowego centrum cyberbezpieczeństwa lub zwiększenia jego zdolności, powinno – wspólnie z ECCC – zakupić odpowiednie narzędzia, infrastrukturę lub usługi. Takie państwo członkowskie powinno kwalifikować się do otrzymania dotacji na obsługę narzędzi, infrastruktury lub usług. Konsorcjum przyjmujące, składające się z co najmniej trzech państw członkowskich, które zostało wybrane przez ECCC w następstwie zaproszenia do wyrażenia zainteresowania w celu ustanowienia transgranicznego centrum cyberbezpieczeństwa lub zwiększenia jego zdolności powinno wspólnie z ECCC zakupić odpowiednie narzędzia, infrastrukturę lub usługi. Konsorcjum przyjmujące powinno kwalifikować się do otrzymania dotacji na obsługę narzędzi, infrastruktury lub usług. Postępowanie o udzielenie zamówienia mające na celu zakup odpowiednich narzędzi, infrastruktury lub usług powinno być przeprowadzone wspólnie przez ECCC i właściwe instytucje zamawiające z państw członkowskich wybranych w następstwie takich zaproszeń do wyrażenia zainteresowania. Takie postępowanie powinno być zgodne z art. 168 ust. 2 rozporządzenia (UE, Euratom) 2024/2509 oraz zasadami finansowymi ECCC. Podmioty prywatne nie powinny zatem kwalifikować się do udziału w zaproszeniach do wyrażenia zainteresowania dotyczących wspólnego z ECCC zakupu narzędzi, infrastruktury lub usług ani do otrzymywania dotacji na obsługę tych narzędzi, infrastruktury i usług. Państwa członkowskie powinny jednak móc angażować podmioty prywatne w tworzenie, ulepszanie i funkcjonowanie swoich krajowych centrów cyberbezpieczeństwa i transgranicznych centrów cyberbezpieczeństwa w inny sposób, który uznają za stosowny, zgodnie z prawem Unii i prawem krajowym. Podmioty prywatne mogą również kwalifikować się do otrzymania finansowania unijnego zgodnie z rozporządzeniem (UE) 2021/887 w celu udzielenia wsparcia krajowym centrom cyberbezpieczeństwa.

(17) Aby zwiększyć wykrywanie cyberzagrożeń oraz orientację sytuacyjną w Unii, państwo członkowskie wybrane w następstwie zaproszenia do wyrażenia zainteresowania w celu utworzenia krajowego centrum cyberbezpieczeństwa lub zwiększenia jego zdolności powinno zobowiązać się do złożenia wniosku o uczestnictwo w transgranicznym centrum cyberbezpieczeństwa. Jeżeli państwo członkowskie nie przyłączy się do transgranicznego centrum cyberbezpieczeństwa w ciągu dwóch lat od daty nabycia narzędzi, infrastruktury lub usług lub od daty otrzymania finansowania w formie dotacji, w zależności od tego, co nastąpiło wcześniej, nie powinno kwalifikować się do udziału w dodatkowych unijnych działaniach wspierających w ramach europejskiego systemu cyberostrzeżeń służących zwiększeniu zdolności jego krajowego centrum cyberbezpieczeństwa. W takich przypadkach podmioty z państw członkowskich mogą nadal uczestniczyć w zaproszeniach do składania wniosków dotyczących innych tematów w ramach programu „Cyfrowa Europa" lub innych unijnych programów finansowania, w tym w zaproszeniach do składania wniosków dotyczących zdolności w zakresie wykrywania cyberataków i udostępniania informacji, pod warunkiem że podmioty te spełniają kryteria kwalifikowalności określone w tych programach.

(18) CSIRT wymieniają informacje w ramach sieci CSIRT zgodnie z dyrektywą (UE) 2022/2555. Europejski system cyberostrzeżeń powinien stanowić nową zdolność, która jest uzupełnieniem sieci CSIRT i przyczynia się do budowania unijnej orientacji sytuacyjnej umożliwiającej wzmocnienie jej zdolności. Transgraniczne centra cyberbezpieczeństwa powinny działać w ścisłej koordynacji i współpracy z siecią CSIRT. Ich działalność powinna obejmować łączenie danych i udostępnianie odpowiednich informacji, w stosownych przypadkach zanonimizowanych, na temat cyberzagrożeń od podmiotów publicznych i prywatnych, zwiększanie wartości takich danych i informacji dzięki analizie eksperckiej oraz wspólnie nabytym infrastrukturze i najnowocześniejszym narzędziom oraz przyczynianie się do suwerenności technologicznej Unii, jej otwartej strategicznej autonomii, konkurencyjności i odporności, a także wkład w rozwój zdolności Unii.

(19) Transgraniczne centra cyberbezpieczeństwa powinny działać jako centralne punkty, które umożliwiają szeroko zakrojone łączenie odpowiednich danych, w tym danych wywiadowczych na temat cyberzagrożeń, oraz pozwalają na rozpowszechnianie informacji o zagrożeniach wśród dużej i zróżnicowanej grupy zainteresowanych stron, takich jak zespoły reagowania na incydenty komputerowe (CERT), CSIRT, ISAC i operatorzy infrastruktury krytycznej. Członkowie konsorcjum przyjmującego powinni określić w umowie konsorcjum odpowiednie informacje, które mają być udostępniane między uczestnikami danego transgranicznego centrum cyberbezpieczeństwa. Informacje wymieniane między uczestnikami transgranicznego centrum cyberbezpieczeństwa mogłyby obejmować na przykład dane z sieci i czujników, dane wywiadowcze o zagrożeniach, oznaki naruszenia integralności oraz informacje kontekstowe na temat incydentów, cyberzagrożeń, potencjalnych zdarzeń dla cyberbezpieczeństwa i podatności,

([12]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/887 z dnia 20 maja 2021 r. ustanawiające Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa oraz sieć krajowych ośrodków koordynacji (Dz.U. L 202 z 8.6.2021, s. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

technik i procedur oraz wrogich taktyk, konkretne informacje o agresorach, cyberostrzeżenia i zalecenia dotyczące konfiguracji narzędzi cyberbezpieczeństwa służących wykrywaniu cyberataków. Ponadto transgraniczne centra cyberbezpieczeństwa powinny również zawierać między sobą umowy o współpracy. Takie umowy o współpracy powinny w szczególności określać zasady udostępniania informacji i interoperacyjności. Wzorem i punktem wyjścia dla zawartych w nich klauzuli dotyczących interoperacyjności, w szczególności formatów udostępniania i protokołów wymiany informacji, powinny być wytyczne dotyczące interoperacyjności wydane przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) ustanowioną rozporządzeniem (UE) 2019/881. Wytyczne te powinny zostać szybko wydane, aby zapewnić możliwość ich uwzględnienia przez transgraniczne centra cyberbezpieczeństwa na wczesnym etapie. Należy w nich uwzględnić międzynarodowe standardy i najlepsze praktyki oraz sposób funkcjonowania istniejących transgranicznych centrów cyberbezpieczeństwa.

(20) Transgraniczne centra cyberbezpieczeństwa i sieć CSIRT powinny ściśle ze sobą współpracować, aby zapewnić synergię i komplementarność działań. W tym celu powinny one uzgodnić procedury dotyczące współpracy i udostępniania odpowiednich informacji. Może to obejmować udostępnianie odpowiednich informacji na temat cyberzagrożeń i poważnych incydentów w cyberbezpieczeństwie oraz zapewnienie, aby doświadczenia związane z wykorzystaniem przez transgraniczne centra cyberbezpieczeństwa najnowocześniejszych narzędzi, w szczególności sztucznej inteligencji i technologii analityki danych, były udostępniane sieci CSIRT.

(21) Wspólna orientacja sytuacyjna wśród odpowiednich organów jest warunkiem koniecznym gotowości i koordynacji w całej Unii w odniesieniu do poważnych incydentów w cyberbezpieczeństwie i incydentów w cyberbezpieczeństwie na dużą skalę. Dyrektywą (UE) 2022/2555 ustanowiono EU-CyCLONe, aby pomagać w skoordynowanym zarządzaniu na poziomie operacyjnym incydentami i sytuacjami kryzysowymi w cyberbezpieczeństwie na dużą skalę oraz zapewniać regularną wymianę odpowiednich informacji między państwami członkowskimi a instytucjami, organami i jednostkami organizacyjnymi Unii. Dyrektywą (UE) 2022/2555 ustanowiono również sieć CSIRT mającą na celu promowanie szybkiej i skutecznej współpracy operacyjnej między wszystkimi państwami członkowskimi. Aby zapewnić orientację sytuacyjną oraz zwiększyć poziom solidarności w sytuacjach, w których transgraniczne centra cyberbezpieczeństwa uzyskują informacje dotyczące potencjalnego lub trwającego incydentu w cyberbezpieczeństwie na dużą skalę, powinny one przekazywać odpowiednie informacje sieci CSIRT oraz – w ramach wczesnego ostrzegania – EU-CyCLONe. W szczególności, w zależności od sytuacji, udostępniane informacje mogą obejmować informacje techniczne, informacje na temat charakteru i motywów sprawcy lub potencjalnego sprawcy ataku oraz informacje nietechniczne wyższego poziomu na temat potencjalnego lub trwającego incydentu w cyberbezpieczeństwie na dużą skalę. W tym kontekście należy zwrócić należytą uwagę na zasadę ograniczonego dostępu oraz potencjalnie poufny charakter udostępnianych informacji. W dyrektywie (UE) 2022/2555 przypomniano również o odpowiedzialności Komisji w ramach Unijnego Mechanizmu Ochrony Ludności (UMOL) ustanowionego decyzją Parlamentu Europejskiego i Rady 1313/2013/UE ([13]) oraz o jej odpowiedzialności za przedstawianie sprawozdań analitycznych na potrzeby zintegrowanych uzgodnień UE dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych (zwanych dalej „uzgodnieniami IPCR") zgodnie z decyzją wykonawczą Rady (UE) 2018/1993 ([14]). W przypadku gdy transgraniczne centra cyberbezpieczeństwa udostępniają EU-CyCLONe i sieci CSIRT odpowiednie informacje i wczesne ostrzeżenia dotyczące potencjalnego lub trwającego incydentu w cyberbezpieczeństwie na dużą skalę, konieczne jest, aby informacje te były udostępniane za pośrednictwem tych sieci organom państw członkowskich oraz Komisji. W tym kontekście dyrektywa (UE) 2022/2555 przewiduje, że EU-CyCLONe ma za zadanie pomagać w skoordynowanym zarządzaniu na poziomie operacyjnym incydentami i kryzysami w cyberbezpieczeństwie na dużą skalę oraz zapewniać regularną wymianę odpowiednich informacji między państwami członkowskimi a instytucjami, organami i jednostkami organizacyjnymi Unii. Do zadań EU-CyCLONe należy opracowanie wspólnej orientacji sytuacyjnej w odniesieniu do takich incydentów i kryzysów. Jest niezwykle ważne, aby EU-CyCLONe zapewniło, zgodnie z tym celem i zadaniami, aby takie informacje były natychmiast udostępniane odpowiednim przedstawicielom państw członkowskich i Komisji. W tym celu istotne jest, aby regulamin wewnętrzny EU-CyCLONe zawierał odpowiednie przepisy.

(22) Podmioty uczestniczące w europejskim systemie cyberostrzeżeń powinny zapewniać wysoki poziom interoperacyjności między sobą, w tym w stosownych przypadkach w odniesieniu do formatów danych, taksonomii, narzędzi przetwarzania i analityki danych. Powinny one również zapewnić bezpieczne kanały komunikacji, minimalny poziom bezpieczeństwa warstwy aplikacji, tablicę wskaźników orientacji sytuacyjnej oraz same wskaźniki. Przy przyjmowaniu wspólnej taksonomii i opracowywaniu wzoru sprawozdań sytuacyjnych na potrzeby opisywania przyczyn wykrytych cyberzagrożeń i ryzyka w cyberprzestrzeni należy uwzględnić dotychczasowe prace w kontekście wykonywania dyrektywy (UE) 2022/2555.

([13]) Decyzja Parlamentu Europejskiego i Rady nr 1313/2013/UE z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Dz.U. L 347 z 20.12.2013, s. 924, ELI: http://data.europa.eu/eli/dec/2013/1313/oj).

([14]) Decyzja wykonawcza Rady (UE) 2018/1993 z dnia 11 grudnia 2018 r. w sprawie zintegrowanych uzgodnień UE dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych (Dz.U. L 320 z 17.12.2018, s. 28, ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).

(23) Aby umożliwić prowadzoną na dużą skalę wymianę odpowiednich danych i informacji na temat cyberzagrożeń pochodzących z różnych źródeł w zaufanym i bezpiecznym środowisku, podmioty uczestniczące w europejskim systemie cyberostrzeżeń powinny być wyposażone w najnowocześniejsze i wysoce bezpieczne narzędzia, sprzęt i infrastrukturę oraz posiadać wykwalifikowany personel. Powinno to umożliwić poprawę zdolności zbiorowego wykrywania incydentów oraz terminowe ostrzeganie organów i odpowiednich podmiotów, w szczególności dzięki wykorzystaniu najnowszych technologii sztucznej inteligencji i analityki danych.

(24) Dzięki zbieraniu, analizie, udostępnianiu i wymianie odpowiednich danych i informacji europejski system cyberostrzeżeń powinien zwiększać suwerenność technologiczną i otwartą autonomię strategiczną w dziedzinie cyberbezpieczeństwa oraz konkurencyjność i odporność Unii. Łączenie wyselekcjonowanych danych wysokiej jakości może również przyczynić się do rozwoju zaawansowanych narzędzi sztucznej inteligencji i analityki danych. Skuteczne łączenie wysokiej jakości danych wymaga nadzoru człowieka, a zatem wykwalifikowanej siły roboczej.

(25) Chociaż europejski system cyberostrzeżeń jest projektem cywilnym, społeczność zajmująca się cyberobroną mogłaby skorzystać na poprawie cywilnych zdolności w zakresie wykrywania i orientacji sytuacyjnej do celów ochrony infrastruktury krytycznej.

(26) Udostępnianie informacji między uczestnikami europejskiego systemu cyberostrzeżeń powinno być zgodne z obowiązującymi wymogami prawnymi, w szczególności z unijnymi i krajowymi przepisami o ochronie danych, a także z unijnymi regułami konkurencji regulującymi wymianę informacji. Odbiorca informacji powinien wdrożyć – o ile konieczne jest przetwarzanie danych osobowych – środki techniczne i organizacyjne chroniące prawa i wolności osób, których dane dotyczą, oraz zniszczyć dane, gdy tylko przestaną one być niezbędne do określonego celu, oraz poinformować jednostkę udostępniającą dane o ich zniszczeniu.

(27) Zachowanie poufności i bezpieczeństwa informacji ma zasadnicze znaczenie z punktu widzenia wszystkich trzech filarów niniejszego rozporządzenia: zachęcania do udostępniania informacji lub ich wymiany w kontekście europejskiego systemu cyberostrzeżeń, ochrony interesów podmiotów ubiegających się o wsparcie z mechanizmu cyberkryzysowego, lub zapewniania, aby zgłoszenia w ramach europejskiego mechanizmu przeglądu incydentów w cyberbezpieczeństwie umożliwiały zdobycie doświadczenia bez wywierania negatywnego wpływu na podmioty dotknięte incydentami. Udział państw członkowskich i podmiotów w tych mechanizmach wymaga wzajemnego zaufania. Udostępnianie informacji, które zgodnie z przepisami unijnymi lub krajowymi mają status informacji poufnych, lub ich wymiana, powinny być ograniczone do tego, co jest istotne i proporcjonalne do celów tej wymiany. Podczas udostępniania informacji lub ich wymiany należy zachować ich poufność oraz chronić bezpieczeństwo i interesy handlowe każdego zainteresowanego podmiotu. Udostępnianie informacji lub ich wymiana na podstawie niniejszego rozporządzenia może się odbywać z wykorzystaniem umów o zachowaniu poufności lub wytycznych dotyczących dystrybucji informacji, takich jak kod poufności TLP. Kod poufności TLP należy rozumieć jako narzędzie służące informowaniu o wszelkich ograniczeniach w dalszym rozpowszechnianiu informacji. Stosują go niemal wszystkie CSIRT i niektóre ISAC. Oprócz tych ogólnych wymogów, jeżeli chodzi o europejski system cyberostrzeżeń, w umowach konsorcjów przyjmujących należy szczegółowo określić przepisy dotyczące warunków udostępniania informacji w ramach danego transgranicznego centrum cyberbezpieczeństwa. Umowy te mogłyby w szczególności zawierać wymóg, aby udostępnianie informacji odbywało się tylko zgodnie z prawem Unii i prawem krajowym.

(28) Jeśli chodzi o uruchamianie rezerwy cyberbezpieczeństwa UE, konieczne są szczegółowe zasady poufności. Wniosek o wsparcie będzie składany i oceniany, a wsparcie udzielane w kontekście kryzysu podmiotom działającym w sektorach wrażliwych. Aby rezerwa cyberbezpieczeństwa UE mogła skutecznie funkcjonować, użytkownicy i podmioty powinni niezwłocznie udostępniać wszelkie informacje niezbędne do tego, aby każdy podmiot mógł odegrać wyznaczoną mu rolę w ocenie wniosków i uruchamianiu wsparcia. W związku z tym niniejsze rozporządzenie powinno stanowić, że wszystkie takie informacje mogą być wykorzystywane lub udostępniane wyłącznie wtedy, gdy jest to konieczne dla działania rezerwy cyberbezpieczeństwa UE, a informacje poufne lub niejawne na podstawie prawa Unii i prawa krajowego mają być wykorzystywane i udostępniane wyłącznie zgodnie z tym prawem. Ponadto użytkownicy powinni mieć zawsze możliwość, w stosownych przypadkach, skorzystania z protokołów udostępniania informacji, takich jak kody poufności TLP, w celu doprecyzowania ograniczeń. Chociaż użytkownicy mają pewną swobodę w tym względzie, ważne jest, aby przy stosowaniu takich ograniczeń brali pod uwagę możliwe konsekwencje, w szczególności opóźnienie oceny lub wykonania zamówionych usług. Skuteczne funkcjonowanie rezerwy cyberbezpieczeństwa UE wymaga, aby instytucja zamawiająca wyjaśniła użytkownikowi te

konsekwencje przed złożeniem wniosku. Tego typu zabezpieczenia ograniczone są tylko do wniosku i świadczenia usług oferowanych w ramach rezerwy cyberbezpieczeństwa UE oraz nie mają wpływu na wymianę informacji w innych kontekstach, takich jak udzielanie zamówień na potrzeby rezerwy cyberbezpieczeństwa UE.

(29) W związku z rosnącym ryzykiem i rosnącą liczbą incydentów mających wpływ na państwa członkowskie konieczne jest ustanowienie instrumentu wsparcia kryzysowego, a mianowicie mechanizmu cyberkryzysowego, aby poprawić odporność Unii na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę i incydenty równoważne incydentom w cyberbezpieczeństwie na dużą skalę oraz uzupełnić działania państw członkowskich wsparciem finansowym w sytuacjach nadzwyczajnych na potrzeby gotowości, reagowania na incydenty i wstępnego przywrócenia funkcjonowania usług kluczowych. Ponieważ pełne usunięcie skutków incydentu jest kompleksowym procesem przywracania funkcjonowania podmiotu dotkniętego incydentem do stanu sprzed incydentu i może długo trwać oraz pociągać za sobą znaczące koszty, wsparcie z rezerwy cyberbezpieczeństwa UE powinno się ograniczać do wstępnego etapu procesu usuwania skutków, który pomaga przywrócić podstawowe funkcje systemów. Mechanizm cyberkryzysowy powinien umożliwiać szybkie i skuteczne udzielanie pomocy w określonych okolicznościach i na jasnych warunkach oraz dokładne monitorowanie i ocenę sposobu wykorzystania zasobów. O ile podstawowa odpowiedzialność za zapobieganie incydentom i kryzysom spoczywa na państwach członkowskich, mechanizm cyberkryzysowy propaguje solidarność między państwami członkowskimi zgodnie z art. 3 ust. 3 Traktatu o Unii Europejskiej (TUE).

(30) Mechanizm cyberkryzysowy powinien zapewniać państwom członkowskim wsparcie uzupełniające ich własne środki i zasoby oraz inne istniejące możliwości wsparcia w przypadku reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę oraz wstępnego usuwania ich skutków, takie jak: usługi świadczone przez ENISA zgodnie z jej mandatem, skoordynowana reakcja i pomoc ze strony sieci CSIRT, wsparcie ze strony EU-CyCLONe na potrzeby zmniejszenia zagrożeń, a także wzajemna pomoc między państwami członkowskimi, w tym w kontekście art. 42 ust. 7 TUE i zespoły szybkiego reagowania na cyberincydenty w ramach stałej współpracy strukturalnej (PESCO) ustanowione na podstawie decyzji Rady (WPZiB) 2017/2315 ([15]). W mechanizmie tym należy uwzględnić potrzebę zapewnienia dostępności specjalistycznych środków wspierających gotowość, reagowanie na takie incydenty i usuwanie ich skutków w całej Unii i w państwach trzecich stowarzyszonych z programem „Cyfrowa Europa".

(31) Niniejsze rozporządzenie pozostaje bez uszczerbku dla procedur i ram koordynowania reagowania kryzysowego na poziomie Unii, w szczególności dyrektywy (UE) 2022/2555, Unijnego Mechanizmu Ochrony Ludności ustanowionego decyzją Parlamentu Europejskiego i Rady nr 1313/2013/UE ([16]), uzgodnień IPCR oraz zalecenia Komisji (UE) 2017/1584 ([17]). Wsparcie z mechanizmu cyberkryzysowego może uzupełniać pomoc udzielaną w kontekście wspólnej polityki zagranicznej i bezpieczeństwa oraz wspólnej polityki bezpieczeństwa i obrony, w tym za pośrednictwem zespołów szybkiego reagowania na cyberincydenty, uwzględniając cywilny charakter mechanizmu cyberkryzysowego. Wsparcie z mechanizmu cyberkryzysowego może uzupełniać działania realizowane w kontekście art. 42 ust. 7 Traktatu UE, w tym pomoc udzielaną przez jedno państwo członkowskie innemu państwu członkowskiemu, lub stanowić część wspólnej reakcji Unii i państw członkowskich, lub w sytuacjach, o których mowa w art. 222 TFUE. Wykonywanie tego rozporządzenia powinno być również skoordynowane, w stosownych przypadkach, z wdrażaniem środków z zestawu narzędzi dla dyplomacji cyfrowej.

(32) Wsparcie udzielane na podstawie niniejszego rozporządzenia powinno wspomagać i uzupełniać działania podejmowane przez państwa członkowskie na poziomie krajowym. W tym celu należy zapewnić ścisłą współpracę i konsultacje między Komisją, ENISA, państwami członkowskimi oraz, w stosownych przypadkach, ECCC. Wnioskując o wsparcie w ramach mechanizmu cyberkryzysowego, państwo członkowskie powinno przedstawić odpowiednie informacje uzasadniające potrzebę wsparcia.

(33) W dyrektywie (UE) 2022/2555 zobowiązano państwa członkowskiego do wyznaczenia lub ustanowienia co najmniej jednego organu ds. zarządzania kryzysowego w cyberbezpieczeństwie oraz do zapewnienia tym organom odpowiednich zasobów, aby organy te mogły efektywnie i skutecznie wykonywać powierzone im zadania. Zobowiązano w niej również państwa członkowskie do określenia zdolności, zasobów i procedur, które można wykorzystać w razie sytuacji kryzysowej, a także do przyjęcia krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę, w którym określa się cele i tryb zarządzania incydentami i zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę. Państwa członkowskie są również zobowiązane do ustanowienia co najmniej jednego CSIRT, który jest odpowiedzialny za obsługę incydentów zgodnie z wyraźnie

([15]) Decyzja Rady (WPZiB) 2017/2315 z dnia 11 grudnia 2017 r. w sprawie ustanowienia stałej współpracy strukturalnej (PESCO) oraz ustalenia listy uczestniczących w niej państw członkowskich (Dz.U. L 331 z 14.12.2017, s. 57, ELI: http://data.europa.eu/eli/dec/2017/2315/oj).

([16]) Decyzja Parlamentu Europejskiego i Rady nr 1313/2013/UE z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Dz.U. L 347 z 20.12.2013, s. 924).

([17]) Zalecenie Komisji (UE) 2017/1584 z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę (Dz.U. L 239 z 19.9.2017, s. 36).

określoną procedurą i obejmuje co najmniej sektory, podsektory i rodzaje podmiotów wchodzące w zakres stosowania tej dyrektywy, oraz do zapewnienia, aby CSIRT dysponowały odpowiednimi zasobami, tak aby mogły skutecznie realizować swoje zadania. Niniejsze rozporządzenie pozostaje bez uszczerbku dla roli Komisji w zapewnianiu przestrzegania przez państwa członkowskie obowiązków wynikających z dyrektywy (UE) 2022/2555. Mechanizm cyberkryzysowy powinien zapewniać pomoc w zakresie działań mających na celu zwiększenie gotowości, a także działań w zakresie reagowania na incydenty w celu złagodzenia skutków poważnych incydentów w cyberbezpieczeństwie i incydentów w cyberbezpieczeństwie na dużą skalę, wsparcia wstępnego usuwania ich skutków lub przywrócenia podstawowych funkcji usług świadczonych przez podmioty działające w sektorach kluczowych lub podmioty działające w innych sektorach krytycznych.

(34) Aby propagować spójne podejście oraz zwiększyć bezpieczeństwo w całej Unii i na jej rynku wewnętrznym, w ramach działań w zakresie gotowości należy w skoordynowany sposób wspierać testowanie i ocenę cyberbezpieczeństwa podmiotów działających w sektorach kluczowych określonych zgodnie z dyrektywą (UE) 2022/2555, w tym za pomocą ćwiczeń i szkoleń. W tym celu Komisja, po konsultacjach z ENISA, we współpracy z grupą współpracy NIS i EU-CyCLONe, powinna regularnie identyfikować odpowiednie sektory lub podsektory, które powinny kwalifikować się do otrzymania wsparcia finansowego na skoordynowane testowanie gotowości na poziomie Unii. Sektory lub podsektory należy wybierać spośród sektorów kluczowych wymienionych w załączniku I do dyrektywy (UE) 2022/2555. Skoordynowane testowanie gotowości powinno opierać się na wspólnych scenariuszach ryzyka i wspólnych metodykach. Przy wyborze sektorów i opracowywaniu scenariuszy ryzyka należy uwzględnić odpowiednie ogólnounijne oceny ryzyka i scenariusze ryzyka, w tym potrzebę unikania powielania działań, między innymi ocenę ryzyka i scenariusze ryzyka, o które zaapelowano w konkluzjach Rady o rozwijaniu pozycji Unii Europejskiej w kwestiach cyberprzestrzeni i które przeprowadziła Komisja, Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa (zwany dalej „Wysokim Przedstawicielem") i grupa współpracy NIS, w koordynacji z odpowiednimi organami i agencjami cywilnymi i wojskowymi oraz ustanowionymi sieciami, w tym EU-CyCLONe, a także ocenę ryzyka związanego z sieciami i infrastrukturą łączności, o którą to ocenę zaapelowano we wspólnym ministerialnym wezwaniu z Nevers i którą przeprowadziła grupa współpracy NIS przy wsparciu Komisji i ENISA oraz we współpracy z Organem Europejskich Regulatorów Łączności Elektronicznej ustanowionym rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2018/1971 ([18]), skoordynowane na poziomie Unii szacowanie ryzyka krytycznych łańcuchów dostaw, które mają zostać przeprowadzone zgodnie z art. 22 dyrektywy (UE) 2022/2555, oraz testowanie operacyjnej odporności cyfrowej przewidziane w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2022/2554 ([19]). Przy wyborze sektorów należy również uwzględnić zalecenie Rady w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej.

(35) Ponadto w ramach mechanizmu cyberkryzysowego należy udzielać wsparcia dla innych działań w zakresie gotowości oraz wspierać gotowość w innych sektorach, nieobjętych skoordynowanym testowaniem gotowości podmiotów działających w sektorach kluczowych lub podmiotów działających w innych sektorach krytycznych. Działania te mogą obejmować różnego rodzaju działania krajowe związane z gotowością.

(36) W przypadku gdy państwa członkowskie otrzymują dotacje na wsparcie działań w zakresie gotowości, podmioty w sektorach kluczowych mogą uczestniczyć w tych działaniach na zasadzie dobrowolności. Aby w jak największym stopniu wykorzystać działania w zakresie gotowości, dobrą praktyką jest sporządzenie planu środków zaradczych przez uczestniczące w nich podmioty w celu wdrożenia ewentualnych zaleceń dotyczących konkretnych środków. Chociaż ważne jest, aby państwa członkowskie zwróciły się do uczestniczących podmiotów o sporządzenie i wdrożenie takich planów środków zaradczych, niniejsze rozporządzenie nie zobowiązuje państw członkowskich ani nie upoważnia ich do egzekwowania wymogu sporządzania takich planów. Wnioski o sporządzenie takich planów pozostają bez uszczerbku dla wymogów dotyczących podmiotów i uprawnień nadzorczych właściwych organów zgodnie z dyrektywą (UE) 2022/2555.

(37) Mechanizm cyberkryzysowy powinien również zapewniać wsparcie działań w zakresie reagowania na incydenty w celu złagodzenia skutków poważnych incydentów w cyberbezpieczeństwie, incydentów w cyberbezpieczeństwie na dużą skalę i incydentów równoważnych incydentom w cyberbezpieczeństwie na dużą skalę, wsparcia wstępnego usuwania ich skutków lub przywrócenia funkcjonowania usług kluczowych. W stosownych przypadkach powinien on uzupełniać UMOL, aby zapewnić kompleksowe podejście do reagowania na skutki incydentów dla obywateli.

([18]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1971 z dnia 11 grudnia 2018 r. ustanawiające Organ Europejskich Regulatorów Łączności Elektronicznej (BEREC) oraz Agencję Wsparcia BEREC (Urząd BEREC), zmieniające rozporządzenie (UE) 2015/2120 oraz uchylające rozporządzenie (WE) nr 1211/2009 (Dz.U. L 321 z 17.12.2018, s. 1).

([19]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz.U. L 333 z 27.12.2022, s. 1).

(38) Mechanizm cyberkryzysowy powinien wspierać pomoc techniczną udzielaną przez jedno państwo członkowskie drugiemu państwu członkowskiemu dotkniętemu poważnym incydentem w cyberbezpieczeństwie lub incydentem w cyberbezpieczeństwie na dużą skalę, w tym za pośrednictwem sieci CSIRT, o której mowa w art. 11 ust. 3 lit. f) dyrektywy (UE) 2022/2555. Udzielające takiej pomocy państwa członkowskie powinny mieć możliwość składania wniosków o pokrycie kosztów związanych z wysyłaniem zespołów ekspertów w ramach wzajemnej pomocy. Koszty kwalifikowalne mogą obejmować koszty podróży, zakwaterowania i diety dziennej ekspertów ds. cyberbezpieczeństwa.

(39) Biorąc pod uwagę zasadniczą rolę, jaką przedsiębiorstwa prywatne odgrywają w wykrywaniu incydentów w cyberbezpieczeństwie na dużą skalę i incydentów równoważnych incydentom w cyberbezpieczeństwie na dużą skalę oraz w gotowości i reagowaniu na nie, należy uznać wartość dobrowolnej współpracy pro bono z takimi przedsiębiorstwami, w ramach której oferują one bezpłatne usługi w przypadku incydentów i kryzysów w cyberbezpieczeństwie na dużą skalę lub incydentów i kryzysów równoważnych incydentom w cyberbezpieczeństwie na dużą skalę. ENISA, we współpracy z EU-CyCLONe, mogłaby monitorować rozwój takich inicjatyw pro bono oraz promować przestrzeganie przez uczestniczące w nich podmioty kryteriów mających zastosowanie do zaufanych dostawców usług zarządzanych w zakresie bezpieczeństwa na podstawie niniejszego rozporządzenia, w tym w odniesieniu do wiarygodności przedsiębiorstw prywatnych, ich doświadczenia, a także zdolności do bezpiecznego przetwarzania informacji szczególnie chronionych.

(40) W ramach mechanizmu cyberkryzysowego należy stopniowo tworzyć rezerwę cyberbezpieczeństwa UE składającą się z usług oferowanych przez zaufanych dostawców usług zarządzanych w zakresie bezpieczeństwa, aby wspierać reagowanie i wstępne usuwanie skutków w przypadku poważnych incydentów w cyberbezpieczeństwie, incydentów w cyberbezpieczeństwie na dużą skalę lub incydentów równoważnych incydentom w cyberbezpieczeństwie na dużą skalę mających wpływ na państwa członkowskie, instytucje, organy i jednostki organizacyjne Unii lub państwa trzecie stowarzyszone z programem „Cyfrowa Europa". Rezerwa cyberbezpieczeństwa UE powinna zapewniać dostępność i gotowość usług. W związku z tym powinna obejmować usługi, które są deklarowane z wyprzedzeniem, w tym na przykład gotowość do natychmiastowego i szybkiego reagowania. Usługi z rezerwy cyberbezpieczeństwa UE powinny służyć wspieraniu organów krajowych w udzielaniu pomocy dotkniętym incydentami podmiotom działającym w sektorach kluczowych lub dotkniętym incydentami podmiotom działającym w innych sektorach krytycznych jako uzupełnienie działań tych organów na poziomie krajowym. Usługi z rezerwy cyberbezpieczeństwa UE powinny również móc służyć zapewnieniu wsparcia instytucjom, organom i jednostkom organizacyjnym Unii na podobnych warunkach. Rezerwa cyberbezpieczeństwa UE mogłaby także wzmacniać konkurencyjną pozycję przemysłu i usług w Unii w całej gospodarce cyfrowej, w tym mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw, a także przedsiębiorstw typu start-up, w tym poprzez udzielanie zachęt do inwestycji w badania i innowacyjność. Przy zamawianiu usług na potrzeby rezerwy cyberbezpieczeństwa UE ważne jest uwzględnienie europejskich ram umiejętności w dziedzinie cyberbezpieczeństwa ENISA. Wnioskując o wsparcie z rezerwy cyberbezpieczeństwa UE, użytkownicy powinni podać we wniosku odpowiednie informacje na temat dotkniętego incydentem podmiotu i potencjalnych skutków, informacje na temat żądanej usługi z rezerwy cyberbezpieczeństwa UE oraz informacje na temat wsparcia udzielonego na poziomie krajowym podmiotowi dotkniętemu incydentem, które należy uwzględnić przy ocenie wniosku złożonego przez wnioskodawcę. Aby zapewnić komplementarność z innymi formami wsparcia dostępnymi podmiotowi, na który incydent ma wpływ, wniosek powinien także zawierać, w miarę dostępności, informacje o istniejących ustaleniach umownych dotyczących usług reagowania na incydenty i wstępnego usuwania skutków incydentów, a także o umowach ubezpieczeniowych potencjalnie pokrywających koszty takich incydentów.

(41) Aby zapewnić skuteczne wykorzystanie unijnych funduszy, wcześniej zadeklarowane usługi w ramach rezerwy cyberbezpieczeństwa UE należy przekształcić, zgodnie z odpowiednią umową, w usługi w zakresie gotowości związane z zapobieganiem incydentom i reagowaniem na nie, w przypadku gdy takie wcześniej zadeklarowane usługi nie zostaną wykorzystane do reagowania na incydenty w okresie, na który je wcześniej zadeklarowano. Usługi te powinny uzupełniać działania w zakresie gotowości, którymi zarządzać będzie ECCC, a nie powinny ich powielać.

(42) Wnioski o wsparcie z rezerwy cyberbezpieczeństwa UE składane przez organy państw członkowskich ds. zarządzania kryzysowego w cyberbezpieczeństwie oraz CSIRT lub CERT-UE w imieniu instytucji, organów i jednostek organizacyjnych Unii powinna oceniać instytucja zamawiająca. W przypadku gdy ENISA powierzono zarządzanie rezerwą cyberbezpieczeństwa UE i jej obsługę, tą instytucją zamawiającą jest ENISA. Wnioski o wsparcie z rezerwy cyberbezpieczeństwa UE z państw trzecich stowarzyszonych z programem „Cyfrowa Europa" oceniane są przez Komisję. Aby ułatwić składanie i ocenę wniosków o wsparcie, ENISA może utworzyć bezpieczną platformę.

(43) W przypadku otrzymania wielu wniosków równocześnie, porządkuje się je według priorytetów zgodnie z kryteriami określonymi w niniejszym rozporządzeniu. W świetle ogólnych celów niniejszego rozporządzenia kryteria te powinny uwzględniać zakres i dotkliwość incydentu, rodzaj podmiotu, którego dotyczy incydent, potencjalny wpływ incydentu na dotknięte nim państwa członkowskie i użytkowników, potencjalny transgraniczny charakter incydentu oraz ryzyko jego rozprzestrzeniania się, a także środki już podjęte przez użytkownika w reakcji na incydent i wstępnie usunięte skutki. W świetle tych celów oraz biorąc pod uwagę, że wnioski użytkowników

z państw członkowskich mają wyłącznie wspierać w całej Unii podmioty działające w sektorach kluczowych lub podmioty działające w innych sektorach krytycznych, należy nadać wyższy priorytet wnioskom użytkowników z państw członkowskich, w przypadku gdy na podstawie kryteriów równo oceniono dwa lub większą liczbę wniosków. Pozostaje to bez uszczerbku dla wszelkich zobowiązań państw członkowskich, na podstawie odpowiednich umów o przyjęciu, do podejmowania środków na rzecz ochrony i wsparcia instytucji, organów i jednostek organizacyjnych Unii.

(44) Komisja powinna ponosić ogólną odpowiedzialność za wdrożenie rezerwy cyberbezpieczeństwa UE. Biorąc pod uwagę rozległe doświadczenie ENISA w dziedzinie cyberbezpieczeństwa, ENISA jest najbardziej odpowiednią agencją do wdrożenia rezerwy cyberbezpieczeństwa UE. W związku z tym Komisja powinna powierzyć ENISA, częściowo lub – jeżeli uzna to za stosowne – w całości, obsługę rezerwy cyberbezpieczeństwa UE i zarządzanie nią. Powierzenie jej tych zadań powinno się odbyć zgodnie z mającymi zastosowanie przepisami rozporządzenia (UE, Euratom) 2024/2509, a w szczególności powinno być uzależnione od spełnienia odpowiednich warunków podpisania umowy o przyznanie wkładu. Wszelkie aspekty obsługi rezerwy cyberbezpieczeństwa UE i zarządzaniu nią, które nie zostały powierzone ENISA, powinny podlegać zarządzaniu bezpośredniemu przez Komisję, w tym przed podpisaniem umowy o przyznanie wkładu.

(45) Państwa członkowskie powinny odgrywać kluczową rolę w tworzeniu i uruchamianiu rezerwy cyberbezpieczeństwa UE, a także w okresie po jej uruchomieniu. Ponieważ rozporządzenie (UE) 2021/694 jest odpowiednim aktem podstawowym dla działań wdrażających rezerwę cyberbezpieczeństwa UE, działania w ramach rezerwy cyberbezpieczeństwa UE należy uwzględnić w programach prac, o których mowa w art. 24 rozporządzenia (UE) 2021/694. Zgodnie z ust. 6 tego artykułu te programy prac mają być przyjmowane przez Komisję w drodze aktów wykonawczych zgodnie z procedurą sprawdzającą. Ponadto Komisja, w koordynacji z grupą współpracy NIS, powinna określić priorytety i ewolucję rezerwy cyberbezpieczeństwa UE.

(46) Umowy zawarte w ramach rezerwy cyberbezpieczeństwa UE nie powinny wpływać na relacje między przedsiębiorstwami ani na istniejące zobowiązania między podmiotem, na który wpływ ma incydent, lub użytkownikami a dostawcą usług.

(47) Na potrzeby wyboru prywatnych dostawców usług do świadczenia usług w kontekście rezerwy cyberbezpieczeństwa UE konieczne jest ustanowienie zestawu minimalnych kryteriów i wymogów, które należy uwzględnić w zaproszeniu do składania ofert na potrzeby wyboru tych dostawców usług, tak aby zapewnić zaspokojenie potrzeb organów państw członkowskich, podmiotów działających w sektorach kluczowych lub podmiotów działających w innych sektorach krytycznych. Aby zaspokoić szczególne potrzeby państw członkowskich instytucja zamawiająca powinna – w stosownych przypadkach – w momencie przygotowywania zamówienia na usługi na potrzeby rezerwy cyberbezpieczeństwa UE opracować kryteria wyboru i wymogi dodatkowe w stosunku do tych określonych w niniejszym rozporządzeniu. Ważne jest, aby do udziału zachęcać mniejszych dostawców działających na poziomie regionalnym i lokalnym.

(48) Przy wyborze dostawców na potrzeby rezerwy cyberbezpieczeństwa UE instytucja zamawiająca powinna dążyć do tego, aby rezerwa cyberbezpieczeństwa UE, jako całość, obejmowała dostawców, którzy są w stanie spełnić wymogi językowe użytkowników. W tym celu instytucja zamawiająca, przed przygotowaniem specyfikacji warunków zamówienia, powinna zbadać, czy potencjalni użytkownicy rezerwy cyberbezpieczeństwa UE mają szczególne wymogi językowe, tak aby usługi wsparcia z rezerwy cyberbezpieczeństwa UE mogły być świadczone w jednym z języków urzędowych instytucji Unii lub państwa członkowskiego, które będą zrozumiałe dla użytkownika lub podmiotu, którego dotyczy incydent. W przypadku gdy użytkownik wymaga obsługi więcej niż jednego języka do świadczenia usług wsparcia z rezerwy cyberbezpieczeństwa UE, a usługi te zostały zamówione w tych językach dla tego użytkownika, użytkownik ten powinien być w stanie określić we wniosku o wsparcie z rezerwy cyberbezpieczeństwa UE, w którym z języków powinny być świadczone usługi w związku z tym konkretnym incydentem, którego dotyczy wniosek.

(49) Aby wesprzeć ustanowienie rezerwy cyberbezpieczeństwa UE, ważne jest, aby Komisja zwróciła się do ENISA o przygotowanie propozycji programu certyfikacji cyberbezpieczeństwa w odniesieniu do usług zarządzanych w zakresie bezpieczeństwa na podstawie rozporządzenia (UE) 2019/881 w obszarach objętych mechanizmem cyberkryzysowym.

(50) Aby wspierać osiągnięcie celów niniejszego rozporządzenia, które obejmują propagowanie wspólnej orientacji sytuacyjnej, zwiększanie odporności Unii oraz umożliwianie skutecznego reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę, Komisja lub EU-CyCLONe powinny mieć możliwość zwrócenia się do ENISA, ze wsparciem sieci CSIRT i za zgodą danego państwa członkowskiego, o dokonanie przeglądu i oceny cyberzagrożeń, znanych możliwych do wykorzystania podatności oraz działań łagodzących w odniesieniu do konkretnego poważnego incydentu w cyberbezpieczeństwie lub incydentu w cyberbezpieczeństwie na dużą skalę. Po zakończeniu przeglądu i oceny incydentu ENISA powinna przygotować sprawozdanie z przeglądu incydentu we współpracy z zainteresowanym państwem członkowskim, odpowiednimi

zainteresowanymi stronami, w tym z przedstawicielami sektora prywatnego, Komisją oraz innymi odpowiednimi instytucjami, organami i jednostkami organizacyjnymi Unii. Sprawozdanie z przeglądu konkretnych incydentów, sporządzone we współpracy z zainteresowanymi stronami, w tym z sektorem prywatnym, powinno służyć ocenie przyczyn i skutków incydentu po jego wystąpieniu oraz działań łagodzących te skutki. Szczególną uwagę należy zwrócić na spostrzeżenia i doświadczenia przekazywane przez dostawców usług zarządzanych w zakresie bezpieczeństwa, którzy spełniają warunki najwyższej uczciwości zawodowej, bezstronności i wymaganej fachowej wiedzy technicznej zgodnie z wymogami niniejszego rozporządzenia. Sprawozdanie należy dostarczyć EU-CyCLONe, sieci CSIRT i Komisji oraz powinno być ono użyte do wnoszenia wkładu w ich prace, a także w prace ENISA. W przypadku gdy incydent dotyczy państwa trzeciego stowarzyszonego z programem „Cyfrowa Europa", Komisja powinna udostępnić sprawozdanie także Wysokiemu Przedstawicielowi.

(51) Biorąc pod uwagę nieprzewidywalny charakter cyberataków oraz fakt, że często nie są one ograniczone do konkretnego obszaru geograficznego i stwarzają wysokie ryzyko rozprzestrzenienia się, zwiększenie odporności państw sąsiadujących i ich zdolności do skutecznego reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty równoważne incydentom w cyberbezpieczeństwie na dużą skalę przyczynia się do ochrony całej Unii, a szczególnie jej rynku wewnętrznego i przemysłu. Takie działania mogą przyczyniać się do rozwoju dyplomacji cyfrowej Unii. W związku z tym państwa trzecie stowarzyszone z programem „Cyfrowa Europa" powinny móc występować o wsparcie z rezerwy cyberbezpieczeństwa UE, na całości lub części swojego terytorium, w przypadku gdy jest to przewidziane w umowie, na podstawie której dane państwo trzecie jest stowarzyszone z programem „Cyfrowa Europa". Unia powinna wspierać finansowanie dla stowarzyszonych z programem „Cyfrowa Europa" państw trzecich w ramach odpowiednich partnerstw i instrumentów finansowania przeznaczonych dla tych państw. Wsparcie powinno obejmować usługi w obszarze reagowania na poważne incydenty w cyberbezpieczeństwie lub incydenty równoważne incydentom w cyberbezpieczeństwie na dużą skalę oraz wstępnego usuwania skutków takich incydentów.

(52) Warunki określone w niniejszym rozporządzeniu w odniesieniu do rezerwy cyberbezpieczeństwa UE i zaufanych dostawców usług zarządzanych w zakresie bezpieczeństwa powinny mieć zastosowanie do wsparcia udzielanego państwom trzecim stowarzyszonym z programem „Cyfrowa Europa". Państwa trzecie stowarzyszone z programem „Cyfrowa Europa" powinny mieć możliwość wystąpienia o wsparcie z rezerwy cyberbezpieczeństwa UE, w przypadku gdy podmioty, które potrzebują wsparcia z rezerwy cyberbezpieczeństwa UE, są podmiotami działającymi w sektorach kluczowych lub podmiotami działającymi w innych sektorach krytycznych oraz w przypadku gdy wykryte incydenty prowadzą do znaczących zakłóceń operacyjnych lub mogą mieć skutki uboczne w Unii. Państwa trzecie stowarzyszone z programem „Cyfrowa Europa" powinny kwalifikować się do otrzymania wsparcia tylko wtedy, gdy umowa, na podstawie której są one stowarzyszone z programem „Cyfrowa Europa", wyraźnie przewiduje takie wsparcie. Ponadto takie państwa trzecie powinny nadal kwalifikować się do wsparcia tylko tak długo, jak spełnione są trzy kryteria. Po pierwsze, państwo trzecie powinno w pełni przestrzegać odpowiednich postanowień tej umowy. Po drugie, biorąc pod uwagę komplementarny charakter rezerwy cyberbezpieczeństwa UE, państwo trzecie powinno było podjąć odpowiednie kroki, aby przygotować się na poważne incydenty w cyberbezpieczeństwie lub incydenty równoważne incydentom w cyberbezpieczeństwie na dużą skalę. Po trzecie, udzielenie wsparcia z rezerwy cyberbezpieczeństwa UE powinno być spójne z polityką Unii wobec tego państwa i ogólnymi stosunkami z tym państwem oraz z innymi politykami Unii w dziedzinie bezpieczeństwa. W kontekście swojej oceny zgodności z tym trzecim kryterium Komisja powinna konsultować się z Wysokim Przedstawicielem w kwestii dostosowania takiego wsparcia do wspólnej polityki zagranicznej i bezpieczeństwa.

(53) Udzielanie wsparcia państwom trzecim stowarzyszonym z programem „Cyfrowa Europa" może mieć wpływ na stosunki z państwami trzecimi i na politykę bezpieczeństwa Unii, w tym w kontekście wspólnej polityki zagranicznej i bezpieczeństwa oraz wspólnej polityki bezpieczeństwa i obrony. W związku z tym należy przyznać Radzie uprawnienia wykonawcze do zatwierdzania i ustalania okresu, w którym takie wsparcie może być udzielane. Rada powinna działać na podstawie wniosku Komisji, z należytym uwzględnieniem dokonanej przez Komisję oceny trzech kryteriów. To samo powinno mieć zastosowanie do przedłużeń obowiązywania oraz wniosków dotyczących zmiany lub uchylenia takich aktów. W przypadku gdy w wyjątkowych okolicznościach Rada uzna, że nastąpiła istotna zmiana okoliczności w odniesieniu do trzeciego kryterium, Rada powinna mieć możliwość działania z własnej inicjatywy w celu zmiany lub uchylenia aktu wykonawczego bez oczekiwania na wniosek Komisji. Takie istotne zmiany z reguły wymagają pilnych działań, mają szczególnie istotne konsekwencje dla stosunków z państwami trzecimi oraz nie wymagają uprzedniej szczegółowej oceny ze strony Komisji. Ponadto Komisja powinna współpracować z Wysokim Przedstawicielem w odniesieniu do wniosków o wsparcie od państw trzecich stowarzyszonych z programem „Cyfrowa Europa" oraz wdrażania wsparcia przyznanego takim państwom trzecim. Komisja powinna również uwzględniać wszelkie opinie przekazane przez ENISA w odniesieniu do takich wniosków i wsparcia. Komisja powinna informować Radę o wynikach oceny wniosków, w tym o odpowiednich ustaleniach poczynionych w tym względzie, oraz o wdrożonych usługach.

(54) W komunikacie Komisji z dnia 18 kwietnia 2023 r. w sprawie Akademii Umiejętności w dziedzinie Cyberbezpieczeństwa zwrócono uwagę na niedobór wykwalifikowanych specjalistów. Takie kwalifikacje są potrzebne do realizacji celów niniejszego rozporządzenia. Unia pilnie potrzebuje specjalistów posiadających umiejętności i kompetencje, aby zapobiegać cyberatakom, wykrywać i powstrzymywać je oraz bronić Unii, w tym jej najbardziej krytycznej infrastruktury, przed takimi atakami oraz zapewnić jej odporność. W tym celu należy zachęcać do współpracy zainteresowane strony, w tym z sektora prywatnego, środowiska akademickiego i sektora publicznego. Równie ważne jest tworzenie synergii na wszystkich terytoriach Unii w odniesieniu do inwestycji w kształcenie i szkolenie, aby promować tworzenie zabezpieczeń zapobiegających drenażowi mózgów lub powiększeniu luki kompetencyjnej w niektórych regionach bardziej niż w innych. Należy pilnie zlikwidować lukę kompetencyjną w zakresie cyberbezpieczeństwa, a w szczególności zmniejszyć dysproporcję kobiet i mężczyzn w zawodach związanych z cyberbezpieczeństwem, aby promować obecność i udział kobiet w projektowaniu administracji cyfrowej.

(55) Aby pobudzić innowacje na jednolitym rynku cyfrowym, należy wzmocnić badania naukowe i innowacje w dziedzinie cyberbezpieczeństwa w celu przyczynienia się do zwiększenia odporności państw członkowskich i otwartej strategicznej autonomii Unii, co jest celem niniejszego rozporządzenia. Synergie mają zasadnicze znaczenie dla wzmocnienia współpracy i koordynacji między różnymi zainteresowanymi stronami, w tym z sektora prywatnego, społeczeństwa obywatelskiego i środowiska akademickiego.

(56) Niniejsze rozporządzenie powinno uwzględniać zobowiązanie zapisane we wspólnej deklaracji Parlamentu Europejskiego, Rady i Komisji z dnia 26 stycznia 2022 r. zatytułowanej „Europejska deklaracja praw i zasad cyfrowych w cyfrowej dekadzie" do ochrony interesów demokracji Unii, obywateli, przedsiębiorstw i instytucji publicznych przed ryzykiem w cyberprzestrzeni i cyberprzestępczością, w tym przed naruszaniem ochrony danych oraz kradzieżą tożsamości lub manipulowaniem tożsamością.

(57) W celu uzupełnienia niektórych, innych niż istotne elementów niniejszego rozporządzenia należy przekazać Komisji uprawnienia do przyjmowania aktów zgodnie z art. 290 TFUE w celu określenia rodzajów i liczby służb reagowania wymaganych dla rezerwy cyberbezpieczeństwa UE. Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów, oraz aby konsultacje te prowadzone były zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa ([20]). W szczególności, aby zapewnić Parlamentowi Europejskiemu i Radzie udział na równych zasadach w przygotowaniu aktów delegowanych, instytucje te otrzymują wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich, a eksperci tych instytucji mogą systematycznie brać udział w posiedzeniach grup eksperckich Komisji zajmujących się przygotowaniem aktów delegowanych.

(58) W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia, należy powierzyć Komisji uprawnienia wykonawcze na potrzeby doprecyzowania szczegółowych ustaleń dotyczących przyznawania usług wsparcia z rezerwy cyberbezpieczeństwa UE. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011 ([21]).

(59) Bez uszczerbku dla przepisów dotyczących rocznego budżetu Unii wynikających z traktatów Komisja powinna uwzględniać obowiązki wynikające z niniejszego rozporządzenia przy ocenie potrzeb budżetowych i kadrowych ENISA.

(60) Komisja powinna regularnie przeprowadzać ocenę środków przewidzianych w niniejszym rozporządzeniu. Pierwsza taka ocena powinna mieć miejsce w ciągu pierwszych 2 lat po dniu wejścia w życie niniejszego rozporządzenia, a następnie co najmniej co 4 lata, z uwzględnieniem harmonogramu przeglądu wieloletnich ram finansowych ustanowionych zgodnie z art. 312 TFUE. Komisja powinna przedstawić sprawozdanie z poczynionych postępów Parlamentowi Europejskiemu i Radzie. Aby ocenić poszczególne wymagane elementy, w tym zakres informacji udostępnianych w ramach europejskiego systemu cyberostrzeżeń, Komisja powinna opierać się wyłącznie na informacjach, które są łatwo dostępne lub przekazywane dobrowolnie. Biorąc pod uwagę zmiany geopolityczne oraz w celu zapewnienia ciągłości i dalszego rozwoju środków określonych w niniejszym rozporządzeniu na okres po 2027 r. Komisja powinna ocenić konieczność przydziału odpowiednich środków budżetowych w wieloletnich ramach finansowych na lata 2028–2034.

([20]) Dz.U. L 123 z 12.5.2016, s. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj.

([21]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz.U. L 55 z 28.2.2011, s. 13, ELI: http://data.europa.eu/eli/reg/2011/182/oj).

(61) Ponieważ cele niniejszego rozporządzenia, a mianowicie wzmocnienie konkurencyjnej pozycji przemysłu i usług w Unii w całej gospodarce cyfrowej oraz przyczynienie się do suwerenności technologicznej Unii i jej otwartej autonomii strategicznej w dziedzinie cyberbezpieczeństwa, nie mogą zostać osiągnięte w sposób wystarczający przez państwa członkowskie, natomiast ze względu na ich rozmiary i skutki możliwe jest ich lepsze osiągnięcie na poziomie Unii, może ona podjąć działania zgodnie z zasadą pomocniczości określoną w art. 5 TUE. Zgodnie z zasadą proporcjonalności określoną w tym artykule, niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tych celów,

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I

PRZEPISY OGÓLNE

Artykuł 1

Przedmiot i cele

1. Niniejszym rozporządzeniem ustanawia się środki mające na celu zwiększenie zdolności w Unii w zakresie wykrywania cyberzagrożeń i incydentów oraz przygotowywania się i reagowania na takie cyberzagrożenia i incydenty, w szczególności poprzez ustanowienie:

a) ogólnoeuropejskiej sieci centrów cyberbezpieczeństwa (europejskiego systemu cyberostrzeżeń) w celu zbudowania i wzmocnienia zdolności w zakresie skoordynowanego wykrywania i wspólnej orientacji sytuacyjnej;

b) mechanizmu cyberkryzysowego w celu wsparcia państw członkowskich w przygotowaniu się na poważne incydenty w cyberbezpieczeństwie oraz incydenty w cyberbezpieczeństwie na dużą skalę, w reagowaniu na te incydenty oraz w łagodzeniu i wstępnym usuwaniu ich skutków, oraz w celu wsparcia innych użytkowników w reagowaniu na poważne incydenty w cyberbezpieczeństwie i incydenty równoważne incydentom w cyberbezpieczeństwie na dużą skalę;

c) europejskiego mechanizmu przeglądu incydentów w cyberbezpieczeństwie w celu przeglądu i oceny poważnych incydentów w cyberbezpieczeństwie lub incydentów w cyberbezpieczeństwie na dużą skalę.

2. Niniejsze rozporządzenie służy osiągnięciu ogólnych celów, jakimi są wzmocnienie konkurencyjnej pozycji przemysłu i usług w Unii w całej gospodarce cyfrowej, w tym mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw, a także przedsiębiorstw typu start-up, oraz przyczynienie się do suwerenności technologicznej Unii i otwartej strategicznej autonomii w dziedzinie cyberbezpieczeństwa, w tym poprzez pobudzanie innowacji na jednolitym rynku cyfrowym. Realizacja tych celów opiera się na zapewnieniu większej solidarności na poziomie Unii, wzmocnieniu ekosystemu cyberbezpieczeństwa, zwiększeniu cyberodporności państw członkowskich oraz rozwoju umiejętności, know-how, zdolności i kompetencji pracowników w zakresie cyberbezpieczeństwa.

3. Cele ogólne, o których mowa w ust. 2, osiąga się poprzez realizację następujących celów szczegółowych:

a) wzmocnienie wspólnych unijnych zdolności w zakresie skoordynowanego wykrywania cyberzagrożeń i incydentów oraz poprawa wspólnej orientacji sytuacyjnej w tej dziedzinie;

b) zwiększenie gotowości podmiotów działających w sektorach kluczowych lub podmiotów działających w innych sektorach krytycznych w całej Unii oraz wzmocnienie solidarności dzięki rozwijaniu skoordynowanego testowania gotowości i wzmocnionych zdolności reagowania na poważne incydenty w cyberbezpieczeństwie, incydenty w cyberbezpieczeństwie na dużą skalę lub incydenty równoważne incydentom w cyberbezpieczeństwie na dużą skalę oraz usuwania skutków tych incydentów, w tym możliwości udostępnienia unijnego wsparcia w reagowaniu na incydenty w cyberbezpieczeństwie państwom trzecim stowarzyszonym z programem „Cyfrowa Europa”;

c) zwiększenie odporności Unii oraz przyczynianie się do skutecznej reakcji na incydenty poprzez przegląd i ocenę poważnych incydentów w cyberbezpieczeństwie lub incydentów w cyberbezpieczeństwie na dużą skalę, w tym wyciąganie wniosków ze zdobytych doświadczeń oraz, w stosownych przypadkach, wydawanie zaleceń.

4. Działania w ramach niniejszego rozporządzenia prowadzone są z należytym poszanowaniem kompetencji państw członkowskich i uzupełniają działania prowadzone przez sieć CSIRT, EU-CyCLONe oraz grupę współpracy NIS.

5. Niniejsze rozporządzenie pozostaje bez uszczerbku dla podstawowych funkcji państw członkowskich, w tym zapewnienia integralności terytorialnej państwa, utrzymania porządku publicznego oraz ochrony bezpieczeństwa narodowego. W szczególności bezpieczeństwo narodowe pozostaje w zakresie wyłącznej odpowiedzialności każdego państwa członkowskiego.

6. Udostępnianie informacji lub ich wymiana w ramach niniejszego rozporządzenia, mających zgodnie z przepisami unijnymi lub krajowymi status informacji poufnych, ogranicza się do tego, co jest istotne i proporcjonalne do celów tego udostępniania lub tej wymiany. Podczas udostępniania informacji lub ich wymiany zachowuje się poufność informacji oraz chroni się bezpieczeństwo i interesy handlowe zainteresowanych podmiotów. Nie może się to wiązać z udostępnianiem informacji, których ujawnienie byłoby sprzeczne z podstawowymi interesami państw członkowskich w zakresie bezpieczeństwa narodowego, bezpieczeństwa publicznego lub obronności.

Artykuł 2

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „transgraniczne centrum cyberbezpieczeństwa" oznacza wielokrajową platformę ustanowioną na podstawie pisemnej umowy konsorcjum, która łączy w skoordynowanej strukturze sieciowej krajowe centra cyberbezpieczeństwa z co najmniej trzech państw członkowskich i która ma zwiększyć monitorowanie, wykrywanie i analizę cyberzagrożeń, aby zapobiegać incydentom oraz wspierać generowanie danych wywiadowczych na temat cyberzagrożeń, w szczególności poprzez wymianę odpowiednich danych i informacji, w stosownych przypadkach zanonimizowanych, a także poprzez udostępnianie najnowocześniejszych narzędzi oraz wspólne rozwijanie, w zaufanym środowisku, zdolności w zakresie wykrywania i analizy cyberataków, zapobiegania im i ochrony przed nimi;

2) „konsorcjum przyjmujące" oznacza konsorcjum składające się z uczestniczących państw członkowskich, które zgodziły się stworzyć narzędzia, infrastrukturę lub usługi na potrzeby transgranicznego centrum cyberbezpieczeństwa i jego funkcjonowania oraz wnieść wkład w nabycie tych narzędzi, infrastruktury lub usług;

3) „CSIRT" oznacza CSIRT wyznaczony lub ustanowiony zgodnie z art. 10 dyrektywy (UE) 2022/2555;

4) „podmiot" oznacza podmiot zdefiniowany w art. 6 pkt 38 dyrektywy (UE) 2022/2555;

5) „podmioty działające w sektorach kluczowych" oznaczają rodzaje podmiotów wymienione w załączniku I do dyrektywy (UE) 2022/2555;

6) „podmioty działające w innych sektorach krytycznych" oznaczają rodzaje podmiotów wymienione w załączniku II do dyrektywy (UE) 2022/2555;

7) „ryzyko" oznacza ryzyko zdefiniowane w art. 6 pkt 9 dyrektywy (UE) 2022/2555;

8) „cyberzagrożenie" oznacza cyberzagrożenie zdefiniowane w art. 2 pkt 8 rozporządzenia (UE) 2019/881;

9) „incydent" oznacza incydent zdefiniowany w art. 6 pkt 6 dyrektywy (UE) 2022/2555;

10) „poważny incydent w cyberbezpieczeństwie" oznacza incydent spełniający kryteria określone w art. 23 ust. 3 dyrektywy (UE) 2022/2555;

11) „poważny incydent" oznacza poważny incydent zdefiniowany w art. 3 pkt 8 rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) 2023/2841 ([22]);

12) „incydent w cyberbezpieczeństwie na dużą skalę" oznacza incydent w cyberbezpieczeństwie na dużą skalę zdefiniowany w art. 6 pkt 7 dyrektywy (UE) 2022/2555;

([22]) Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) 2023/2841 z dnia 13 grudnia 2023 r. w sprawie ustanowienia środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach i jednostkach organizacyjnych Unii (Dz.U. L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

13) „incydent równoważny incydentowi w cyberbezpieczeństwie na dużą skalę” oznacza, w przypadku instytucji, organów i jednostek organizacyjnych Unii – poważny incydent, a w przypadku państw trzecich stowarzyszonych z programem „Cyfrowa Europa” – incydent, który powoduje poziom zakłóceń wykraczający poza zdolność reagowania danego państwa trzeciego stowarzyszonego z programem „Cyfrowa Europa”;

14) „państwo trzecie stowarzyszone z programem »Cyfrowa Europa«” oznacza państwo trzecie, które jest stroną umowy z Unią umożliwiającej jego udział w programie „Cyfrowa Europa” zgodnie z art. 10 rozporządzenia (UE) 2021/694;

15) „instytucja zamawiająca” oznacza Komisję lub – w zakresie, w jakim obsługę rezerwy cyberbezpieczeństwa UE i zarządzanie nią powierzono ENISA zgodnie z art. 14 ust. 5 niniejszego rozporządzenia – ENISA;

16) „dostawca usług zarządzanych w zakresie bezpieczeństwa” oznacza dostawcę usług zarządzanych w zakresie bezpieczeństwa zdefiniowanego w art. 6 pkt 40 dyrektywy (UE) 2022/2555;

17) „zaufani dostawcy usług zarządzanych w zakresie bezpieczeństwa” oznaczają dostawców usług zarządzanych w zakresie bezpieczeństwa wybranych do włączenia do rezerwy cyberbezpieczeństwa UE zgodnie z art. 17.

ROZDZIAŁ II

EUROPEJSKI SYSTEM CYBEROSTRZEŻEŃ

Artykuł 3

Ustanowienie europejskiego systemu cyberostrzeżeń

1. Ustanawia się europejski system cyberostrzeżeń – ogólnoeuropejską sieć infrastruktury składającą się z krajowych centrów cyberbezpieczeństwa i transgranicznych centrów cyberbezpieczeństwa, przystępujących na zasadzie dobrowolności – aby wspierać rozwój zaawansowanych zdolności Unii w zakresie wykrywania, analizy i przetwarzania danych w odniesieniu do cyberzagrożeń oraz zapobiegania incydentom w Unii.

2. Europejski system cyberostrzeżeń ma za zadanie:

a) przyczyniać się do lepszej ochrony przed cyberzagrożeniami i reagowania na nie poprzez wspieranie odpowiednich podmiotów, w szczególności CSIRT, sieci CSIRT, EU-CyCLONe i właściwych organów wyznaczonych lub ustanowionych na podstawie art. 8 ust. 1 dyrektywy (UE) 2022/2555, poprzez współpracę z tymi podmiotami i wzmacnianie ich zdolności;

b) gromadzić odpowiednie dane i informacje na temat cyberzagrożeń i incydentów z różnych źródeł w ramach transgranicznych centrów cyberbezpieczeństwa oraz udostępniać przeanalizowane lub zagregowane informacje za pośrednictwem transgranicznych centrów cyberbezpieczeństwa, w stosownych przypadkach z siecią CSIRT;

c) zbierać wysokiej jakości, użyteczne operacyjnie informacje i dane wywiadowcze dotyczące cyberzagrożeń oraz wspierać generowanie tych informacji i danych, z wykorzystaniem najnowocześniejszych narzędzi i zaawansowanych technologii, a także udostępniać te informacje i dane wywiadowcze dotyczące cyberzagrożeń;

d) przyczyniać się do zwiększenia skoordynowanego wykrywania cyberzagrożeń i wspólnej orientacji sytuacyjnej w całej Unii oraz do wydawania ostrzeżeń, w tym, w stosownych przypadkach, poprzez przekazywanie podmiotom konkretnych zaleceń;

e) świadczyć usługi i prowadzić działania na rzecz podmiotów zajmujących się cyberbezpieczeństwem w Unii, w tym przyczyniać się do rozwoju zaawansowanych narzędzi i technologii, takich jak narzędzia sztucznej inteligencji i analityki danych.

3. Działania wdrażające europejski system cyberostrzeżeń wspiera się ze środków programu „Cyfrowa Europa” i realizuje zgodnie z rozporządzeniem (UE) 2021/694, w szczególności zgodnie z jego celem szczegółowym nr 3.

Artykuł 4

Krajowe centra cyberbezpieczeństwa

1. W przypadku gdy państwo członkowskie postanowi uczestniczyć w europejskim systemie cyberostrzeżeń, wyznacza lub, w stosownych przypadkach, ustanawia krajowe centrum cyberbezpieczeństwa do celów niniejszego rozporządzenia.

2. Krajowe centrum cyberbezpieczeństwa jest pojedynczym podmiotem działającym z upoważnienia państwa członkowskiego. Może to być CSIRT lub, w stosownych przypadkach, krajowy organ ds. zarządzania kryzysowego w cyberbezpieczeństwie lub inny właściwy organ wyznaczony lub ustanowiony zgodnie z art. 8 ust. 1 dyrektywy (UE) 2022/2555, lub inny podmiot. Krajowe centrum cyberbezpieczeństwa musi:

a) mieć zdolność do pełnienia funkcji punktu odniesienia i punktu dostępu dla innych organizacji publicznych i prywatnych na poziomie krajowym w celu zbierania i analizowania informacji dotyczących cyberzagrożeń i incydentów oraz wspierania działalności transgranicznego centrum cyberbezpieczeństwa, o którym mowa w art. 5; oraz

b) być w stanie wykrywać, agregować i analizować dane i informacje istotne z punktu widzenia cyberzagrożeń i incydentów, takie jak dane wywiadowcze dotyczące cyberzagrożeń, w szczególności za pomocą najnowocześniejszych technologii, aby zapobiegać incydentom.

3. W ramach funkcji, o których mowa w ust. 2 niniejszego artykułu, krajowe centra cyberbezpieczeństwa mogą współpracować z podmiotami sektora prywatnego w celu wymiany odpowiednich danych i informacji na potrzeby wykrywania cyberzagrożeń i incydentów oraz zapobiegania im, w tym z sektorowymi i międzysektorowymi grupami podmiotów kluczowych i ważnych, o których mowa w art. 3 dyrektywy (UE) 2022/2555. W stosownych przypadkach oraz zgodnie z prawem Unii i prawem krajowym informacje, o które występują lub które otrzymują krajowe centra cyberbezpieczeństwa, mogą obejmować dane telemetryczne, dane z czujników i dane z rejestrów.

4. Państwo członkowskie wybrane na podstawie art. 9 ust. 1 zobowiązuje się do złożenia wniosku o uczestnictwo jego krajowego centrum cyberbezpieczeństwa w transgranicznym centrum cyberbezpieczeństwa.

Artykuł 5

Transgraniczne centra cyberbezpieczeństwa

1. W przypadku gdy co najmniej trzy państwa członkowskie zobowiązują się, aby ich krajowe centra cyberbezpieczeństwa współpracowały ze sobą w celu koordynacji działań w zakresie wykrywania cyberataków i monitorowania zagrożeń, te państwa członkowskie mogą utworzyć konsorcjum przyjmujące do celów niniejszego rozporządzenia.

2. Konsorcjum przyjmujące jest konsorcjum składającym się z co najmniej trzech uczestniczących państw członkowskich, które zgodziły się stworzyć narzędzia, infrastrukturę lub usługi na potrzeby transgranicznego centrum cyberbezpieczeństwa i jego funkcjonowania oraz wnieść wkład w nabycie tych narzędzi, infrastruktury i usług zgodnie z ust. 4.

3. W przypadku wyboru konsorcjum przyjmującego zgodnie z art. 9 ust. 3 jego członkowie zawierają pisemną umowę konsorcjum, która:

a) określa wewnętrzne ustalenia dotyczące wykonania umowy o przyjęciu i użytkowaniu, o której mowa w art. 9 ust. 3;

b) ustanawia transgraniczne centrum cyberbezpieczeństwa konsorcjum przyjmującego; oraz

c) zawiera szczegółowe klauzule wymagane na podstawie art. 6 ust. 1 i 2.

4. Transgraniczne centrum cyberbezpieczeństwa jest wielokrajową platformą ustanowioną na podstawie pisemnej umowy konsorcjum, o której mowa w ust. 3. Skupia ona w ramach skoordynowanej struktury sieciowej krajowe centra cyberbezpieczeństwa państw członkowskich konsorcjum przyjmującego. Transgraniczne centrum cyberbezpieczeństwa ma na celu wzmocnienie monitorowania, wykrywania i analizy cyberzagrożeń, zapobieganie incydentom i wspieranie generowania danych wywiadowczych dotyczących cyberzagrożeń, w szczególności poprzez wymianę odpowiednich danych i informacji,, w stosownych przypadkach zanonimizowanych, a także poprzez udostępnianie najnowocześniejszych narzędzi i wspólne rozwijanie, w zaufanym środowisku, zdolności w zakresie wykrywania i analizy cyberataków, zapobiegania im i ochrony przed nimi.

5. Transgraniczne centrum cyberbezpieczeństwa reprezentowane jest do celów prawnych przez członka odpowiedniego konsorcjum przyjmującego pełniącego funkcję koordynatora lub przez konsorcjum przyjmujące, jeżeli ma ono osobowość prawną. Odpowiedzialność za zgodność transgranicznego centrum cyberbezpieczeństwa z niniejszym rozporządzeniem oraz umową o przyjęciu i użytkowaniu określa pisemna umowa konsorcjum, o której mowa w ust. 3.

6. Państwo członkowskie może przystąpić do istniejącego konsorcjum przyjmującego za zgodą członków tego konsorcjum przyjmującego. W takim przypadku odpowiednio zmienia się pisemną umowę konsorcjum, o której mowa w ust. 3, oraz umowę o przyjęciu i użytkowaniu. Nie ma to wpływu na prawa własności Europejskiego Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa (ECCC) do narzędzi, infrastruktury lub usług już zamówionych wspólnie z tym konsorcjum przyjmującym.

Artykuł 6

Współpraca i udostępnianie informacji w ramach transgranicznych centrów cyberbezpieczeństwa i między nimi

1. Członkowie konsorcjum przyjmującego zapewniają, aby ich krajowe centra cyberbezpieczeństwa, zgodnie z pisemną umową konsorcjum, o której mowa w art. 5 ust. 3, udostępniały w ramach transgranicznego centrum cyberbezpieczeństwa odpowiednie informacje, w stosownych przypadkach zanonimizowane, takie jak informacje o cyberzagrożeniach, potencjalnych zdarzeniach dla cyberbezpieczeństwa, podatnościach, technikach i procedurach, oznakach naruszenia integralności systemu, wrogich taktykach, a także informacjami specyficznymi dla konkretnych agresorów, ostrzeżeniami dotyczącymi cyberbezpieczeństwa i zaleceniami dotyczącymi konfiguracji narzędzi cyberbezpieczeństwa mających wykrywać cyberataki, w przypadku gdy udostępnianie takich informacji:

a) wspiera i usprawnia wykrywanie cyberzagrożeń oraz wzmacnia zdolności sieci CSIRT w zakresie zapobiegania incydentom i reagowania na nie lub łagodzenia ich skutków;

b) zwiększa poziom cyberbezpieczeństwa, na przykład przez podnoszenie świadomości na temat cyberzagrożeń, ograniczanie lub utrudnianie rozprzestrzeniania się cyberzagrożeń, wspieranie różnorodnych zdolności do obrony przed nimi, eliminowanie i ujawnianie podatności, techniki wykrywania zagrożeń, ograniczania ich zasięgu i zapobiegania im, strategie ograniczania ryzyka, etapy reagowania i przywracania normalnego działania lub wspieranie badań nad zagrożeniami prowadzonych w ramach współpracy między podmiotami publicznymi i prywatnymi.

2. Pisemna umowa konsorcjum, o której mowa w art. 5 ust. 3, określa:

a) zobowiązanie do udostępniania wśród członków konsorcjum przyjmującego informacji, o których mowa w ust. 1, oraz warunki udostępniania tych informacji;

b) ramy zarządzania wyjaśniające i zachęcające do udostępniania przez wszystkich uczestników odpowiednich informacji, w stosownych przypadkach zanonimizowanych, o których mowa w ust. 1;

c) cele dotyczące wkładu w rozwój zaawansowanych narzędzi i technologii, takich jak sztuczna inteligencja i narzędzia analityki danych.

Pisemna umowa konsorcjum może przewidywać, że udostępnianie informacji, o których mowa w ust. 1, musi odbywać się zgodnie z prawem Unii i prawem krajowym.

3. Transgraniczne centra cyberbezpieczeństwa zawierają między sobą umowy o współpracy określające zasady interoperacyjności i udostępniania informacji między transgranicznymi centrami cyberbezpieczeństwa. Transgraniczne centra cyberbezpieczeństwa informują Komisję o zawartych umowach o współpracy.

3. Udostępnianie informacji, o których mowa w ust. 1, między transgranicznymi centrami cyberbezpieczeństwa zapewnia się poprzez wysoki poziom interoperacyjności. Aby wspierać taką interoperacyjność, ENISA, w ścisłym porozumieniu z Komisją, bez zbędnej zwłoki i w każdym razie do dnia 5 lutego 2026 r. wyda wytyczne dotyczące interoperacyjności określające w szczególności formaty i protokoły udostępniania informacji, z uwzględnieniem międzynarodowych norm i najlepszych praktyk, a także funkcjonowanie wszelkich ustanowionych transgranicznych centrów cyberbezpieczeństwa. Wymogi w zakresie interoperacyjności przewidziane w umowach o współpracy transgranicznych centrów cyberbezpieczeństwa opierają się na wytycznych wydanych przez ENISA.

Artykuł 7

Współpraca z sieciami unijnymi i udostępnianie im informacji

1. Transgraniczne centra cyberbezpieczeństwa i sieć CSIRT ściśle ze sobą współpracują, w szczególności w celu udostępniania informacji. W tym celu uzgadniają one proceduralne aspekty współpracy i udostępniania odpowiednich informacji oraz, bez uszczerbku dla ust. 2, rodzaje informacji, które mają być udostępniane.

2. W przypadku gdy transgraniczne centra cyberbezpieczeństwa otrzymują informacje na temat potencjalnego lub trwającego incydentu w cyberbezpieczeństwie na dużą skalę, zapewniają one, do celów wspólnej orientacji sytuacyjnej, aby odpowiednie informacje oraz wczesne ostrzeżenia przekazano bez zbędnej zwłoki organom państw członkowskich i Komisji za pośrednictwem EU-CyCLONe i sieci CSIRT.

Artykuł 8

Bezpieczeństwo

1. Państwa członkowskie uczestniczące w europejskim systemie cyberostrzeżeń zapewniają wysoki poziom cyberbezpieczeństwa, w tym poufności i bezpieczeństwa danych, a także bezpieczeństwa fizycznego sieci europejskiego systemu cyberostrzeżeń oraz zapewniają, aby sieć ta była odpowiednio zarządzana i kontrolowana w taki sposób, aby chronić ją przed zagrożeniami oraz zapewnić bezpieczeństwo jej i systemów, w tym bezpieczeństwo danych i informacji udostępnianych za pośrednictwem tej sieci.

2. Państwa członkowskie uczestniczące w europejskim systemie cyberostrzeżeń zapewniają, aby udostępnianie informacji, o których mowa w art. 6 ust. 1, w ramach europejskiego systemu cyberostrzeżeń jakiemukolwiek podmiotowi innemu niż organ lub podmiot publiczny państwa członkowskiego nie wpływało negatywnie na interesy Unii lub państw członkowskich w zakresie bezpieczeństwa.

Artykuł 9

Finansowanie europejskiego systemu cyberostrzeżeń

1. W następstwie zaproszenia do wyrażenia zainteresowania dla państw członkowskich zamierzających uczestniczyć w europejskim systemie cyberostrzeżeń ECCC wybiera państwa członkowskie do udziału, wraz z ECCC, we wspólnych zamówieniach publicznych na narzędzia, infrastrukturę lub usługi w celu utworzenia krajowych centrów cyberbezpieczeństwa wyznaczonych lub ustanowionych zgodnie z art. 4 ust. 1, lub zwiększenia ich zdolności. ECCC może przyznać wybranym państwom członkowskim dotacje na finansowanie funkcjonowania takich narzędzi, infrastruktury lub usług. Wkład finansowy Unii pokrywa do 50 % kosztów nabycia narzędzi, infrastruktury lub usług oraz do 50 % kosztów operacyjnych. Wybrane państwa członkowskie pokrywają pozostałe koszty. Przed rozpoczęciem procedury nabycia narzędzi, infrastruktury lub usług ECCC i wybrane państwa członkowskie zawierają umowę o przyjęciu i użytkowaniu regulującą użytkowanie tych narzędzi, infrastruktury lub usług.

2. W przypadku gdy krajowe centrum cyberbezpieczeństwa państwa członkowskiego nie stanie się uczestnikiem transgranicznego centrum cyberbezpieczeństwa w ciągu 2 lat od dnia nabycia narzędzi, infrastruktury lub usług lub od dnia otrzymania finansowania w formie dotacji, w zależności od tego, co nastąpiło wcześniej, dane państwo członkowskie nie kwalifikuje się do dodatkowego wsparcia unijnego na podstawie niniejszego rozdziału, dopóki nie przystąpi do transgranicznego centrum cyberbezpieczeństwa.

3. W następstwie zaproszenia do wyrażenia zainteresowania ECCC wybiera konsorcjum przyjmujące do udziału, wraz z ECCC, we wspólnym zamówieniu na narzędzia, infrastrukturę lub usługi. ECCC może przyznać konsorcjum przyjmującemu dotację na finansowanie funkcjonowania tych narzędzi, infrastruktury lub usług. Wkład finansowy Unii pokrywa do 75 % kosztów nabycia narzędzi, infrastruktury lub usług oraz do 50 % kosztów operacyjnych. Konsorcjum przyjmujące pokrywa pozostałe koszty. Przed rozpoczęciem procedury nabycia narzędzi, infrastruktury lub usług ECCC i konsorcjum przyjmujące zawierają umowę o przyjęciu i użytkowaniu regulującą użytkowanie tych narzędzi, infrastruktury lub usług.

4. Co najmniej raz na dwa lata ECCC przygotowuje zestawienie niezbędnych narzędzi, infrastruktury lub usług o odpowiedniej jakości do utworzenia lub wzmocnienia zdolności krajowych centrów cyberbezpieczeństwa i transgranicznych centrów cyberbezpieczeństwa oraz ich dostępności, w tym od podmiotów prawnych mających siedzibę lub uznawanych za mające siedzibę w państwach członkowskich i kontrolowanych przez państwa członkowskie lub przez obywateli państw członkowskich. Przygotowując to zestawienie, ECCC konsultuje się z siecią CSIRT, wszelkimi istniejącymi transgranicznymi centrami cyberbezpieczeństwa, ENISA i Komisją.

ROZDZIAŁ III

MECHANIZM CYBERKRYZYSOWY

Artykuł 10

Ustanowienie mechanizmu cyberkryzysowego

1. Ustanawia się mechanizm cyberkryzysowy, aby wspierać poprawę odporności Unii na cyberzagrożenia oraz przygotować się na krótkoterminowe skutki poważnych incydentów w cyberbezpieczeństwie, incydentów w cyberbezpieczeństwie na dużą skalę i incydentów równoważnych incydentom w cyberbezpieczeństwie na dużą skalę oraz łagodzić je w duchu solidarności.

2. W przypadku państw członkowskich działania w ramach mechanizmu cyberkryzysowego podejmowane są na wniosek oraz uzupełniają wysiłki i działania państw członkowskich mające na celu przygotowanie się na incydenty, reagowanie na nie i usuwanie ich skutków.

3. Działania wdrażające mechanizm cyberkryzysowy wspiera się ze środków programu „Cyfrowa Europa" i realizuje zgodnie z rozporządzeniem (UE) 2021/694, w szczególności zgodnie z jego celem szczegółowym nr 3.

4. Działania w ramach mechanizmu cyberkryzysowego realizowane są przede wszystkim za pośrednictwem ECCC zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2021/887. Jednakże działania wdrażające rezerwę cyberbezpieczeństwa UE, o której mowa w art. 10 ust. 1 lit. b) niniejszego rozporządzenia, realizowane są przez Komisję i ENISA.

Artykuł 11

Rodzaje działań

W ramach mechanizmu cyberkryzysowego wspiera się następujące rodzaje działań:

a) działania w zakresie gotowości, a mianowicie:

   (i) skoordynowane testowanie gotowości podmiotów działających w sektorach kluczowych w całej Unii, jak określono w art. 12;

   (ii) inne działania w zakresie gotowości dla podmiotów działających w sektorach kluczowych lub podmiotów działających w innych sektorach krytycznych, jak określono w art. 13;

b) działania wspierające reagowanie na poważne incydenty w cyberbezpieczeństwie, incydenty w cyberbezpieczeństwie na dużą skalę i incydenty równoważne incydentom w cyberbezpieczeństwie na dużą skalę oraz wstępne usuwanie ich skutków, realizowane przez zaufanych dostawców usług zarządzanych w zakresie bezpieczeństwa uczestniczących w rezerwie cyberbezpieczeństwa UE ustanowionej na podstawie art. 14;

c) działania w zakresie wspierania wzajemnej pomocy, o których mowa w art. 18.

Artykuł 12

Skoordynowane testowanie gotowości podmiotów

1. Mechanizm cyberkryzysowy wspiera dobrowolne skoordynowane testowanie gotowości podmiotów działających w sektorach kluczowych.

2. Skoordynowane testowanie gotowości może obejmować działania w zakresie gotowości, takie jak testy penetracyjne i ocena zagrożenia.

3. Wsparcia na rzecz działań w zakresie gotowości na podstawie niniejszego artykułu udziela się państwom członkowskim przede wszystkim w formie dotacji oraz na warunkach określonych w odpowiednich programach prac, o których mowa w art. 24 rozporządzenia (UE) 2021/694.

4. Do celów wspierania w całej Unii skoordynowanego testowania gotowości podmiotów, o których mowa w art. 11 lit. a) ppkt (i) niniejszego rozporządzenia, Komisja, po konsultacji z grupą współpracy NIS, EU-CyCLONe i ENISA, określa odpowiednie sektory lub podsektory spośród sektorów kluczowych wymienionych w załączniku I do dyrektywy

(UE) 2022/2555, dla których może zostać ogłoszone zaproszenie do składania wniosków o przyznanie dotacji. Udział państw członkowskich w takich zaproszeniach do składania wniosków jest dobrowolny.

5. Określając sektory lub podsektory, o których mowa w ust. 4, Komisja bierze pod uwagę skoordynowane oceny ryzyka i testy odporności na poziomie Unii oraz ich wyniki.

6. Grupa współpracy NIS we współpracy z Komisją, Wysokim Przedstawicielem Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa (dalej zwanym „Wysokim Przedstawicielem") i ENISA oraz, w ramach jej mandatu, EU-CyCLONe, opracowuje wspólne scenariusze ryzyka i metodyki na potrzeby skoordynowanego testowania gotowości, o którym mowa w art. 11 lit. a) ppkt (i) oraz, w stosownych przypadkach, innych działań w zakresie gotowości, o których mowa w lit. a) ppkt (ii) tego artykułu.

7. W przypadku gdy podmiot działający w sektorze kluczowym dobrowolnie uczestniczy w skoordynowanym testowaniu gotowości, a wynikiem tego testowania są zalecenia dotyczące konkretnych środków, które podmiot uczestniczący mógłby włączyć do planu działań naprawczych, organ państwa członkowskiego odpowiedzialny za skoordynowane testowanie gotowości dokonuje, w stosownych przypadkach, przeglądu działań podjętych w następstwie tych środków przez podmioty uczestniczące z myślą o zwiększeniu gotowości.

Artykuł 13

Inne działania w zakresie gotowości

1. Mechanizm cyberkryzysowy wspiera działania w zakresie gotowości nieobjęte art. 12. Działania takie obejmują działania w zakresie gotowości dla podmiotów w sektorach, które nie zostały wyznaczone do skoordynowanych testów gotowości zgodnie z art. 12. Takie działania mogą wspierać monitorowanie podatności na zagrożenia, monitorowanie ryzyka, ćwiczenia i szkolenia.

2. Wsparcia na rzecz działań w zakresie gotowości na podstawie niniejszego artykułu udziela się państwom członkowskim na ich wniosek przede wszystkim w formie dotacji oraz na warunkach przewidzianych w odpowiednich programach prac, o których mowa w art. 24 rozporządzenia (UE) 2021/694.

Artykuł 14

Ustanowienie rezerwy cyberbezpieczeństwa UE

1. Ustanawia się rezerwę cyberbezpieczeństwa UE, aby pomóc użytkownikom, o których mowa w ust. 3, na ich wniosek, w reagowaniu lub w udzielaniu wsparcia w reagowaniu na poważne incydenty w cyberbezpieczeństwie, incydenty w cyberbezpieczeństwie na dużą skalę i incydenty równoważne incydentom w cyberbezpieczeństwie na dużą skalę oraz we wstępnym usuwaniu skutków takich incydentów.

2. Rezerwa cyberbezpieczeństwa UE składa się z usług reagowania świadczonych przez zaufanych dostawców usług zarządzanych w zakresie bezpieczeństwa wybranych zgodnie z kryteriami określonymi w art. 17 ust. 2. Rezerwa cyberbezpieczeństwa UE może obejmować wcześniej zadeklarowane usługi. Jeżeli wcześniej zadeklarowane usługi zaufanego dostawcy usług zarządzanych w zakresie bezpieczeństwa nie zostaną wykorzystane do reagowania na incydenty w okresie, na który je wcześniej zadeklarowano, możliwe jest ich przekształcenie w usługi w zakresie gotowości związane z zapobieganiem incydentom i reagowaniem na nie. Rezerwa cyberbezpieczeństwa UE jest możliwa do wprowadzenia na wniosek we wszystkich państwach członkowskich, instytucjach, organach i jednostkach organizacyjnych Unii oraz w państwach trzecich stowarzyszonych z programem „Cyfrowa Europa", o których mowa w art. 19 ust. 1.

3. Użytkownikami usług z rezerwy cyberbezpieczeństwa UE są następujące podmioty:

a) organy państw członkowskich ds. zarządzania kryzysowego w cyberbezpieczeństwie oraz CSIRT, o których mowa odpowiednio w art. 9 ust. 1 i 2 oraz w art. 10 dyrektywy (UE) 2022/2555;

b) CERT-UE, zgodnie z art. 13 rozporządzenia (UE, Euratom) 2023/2841;

c) właściwe organy, takie jak zespoły reagowania na incydenty bezpieczeństwa komputerowego i organy ds. zarządzania kryzysowego w cyberbezpieczeństwie państw trzecich stowarzyszonych z programem „Cyfrowa Europa" zgodnie z art. 19 ust. 8.

4. Komisja ponosi ogólną odpowiedzialność za wdrażanie rezerwy cyberbezpieczeństwa UE. Komisja decyduje o priorytetach i rozwoju rezerwy cyberbezpieczeństwa UE w porozumieniu z grupą współpracy NIS oraz zgodnie z wymogami użytkowników, o których mowa w ust. 3, a także nadzoruje jej wdrażanie oraz zapewnia komplementarność, spójność, synergię i powiązania z innymi działaniami wspierającymi prowadzonymi na podstawie niniejszego

rozporządzenia oraz z innymi działaniami i programami unijnymi. Priorytety te podlegają przeglądowi i, w stosownych przypadkach, zmianie co 2 lata. Komisja informuje Parlament Europejski i Radę o tych priorytetach oraz wszelkich ich przeglądach.

5. Bez uszczerbku dla ogólnej odpowiedzialności Komisji za wdrożenie rezerwy cyberbezpieczeństwa UE, o której mowa w ust. 4 niniejszego artykułu, oraz z zastrzeżeniem umowy o przyznanie wkładu zdefiniowanej w art. 2 pkt 19 rozporządzenia (UE, Euratom) 2024/2509, Komisja powierza ENISA, w całości lub w części, obsługę rezerwy cyberbezpieczeństwa UE i zarządzanie nią. Aspekty, które nie zostały powierzone ENISA, podlegają bezpośredniemu zarządzaniu przez Komisję.

6. Co najmniej raz na dwa 2 ENISA przygotowuje zestawienie usług potrzebnych użytkownikom, o których mowa w ust. 3 lit. a) i b) niniejszego artykułu. Zestawienie to obejmuje również informacje o dostępności takich usług, w tym ze strony podmiotów prawnych mających siedzibę lub uznanych za mające siedzibę w państwach członkowskich i kontrolowanych przez państwa członkowskie lub obywateli państw członkowskich. Opracowując informacje o dostępności usług, ENISA ocenia umiejętności i zdolności unijnych pracowników sektora cyberbezpieczeństwa istotne z perspektywy celów rezerwy cyberbezpieczeństwa UE. Przygotowując zestawienie ENISA konsultuje się z grupą współpracy NIS, EU-CyCLONe, Komisją oraz, w stosownych przypadkach, z Międzyinstytucjonalną Radą ds. Cyberbezpieczeństwa ustanowioną zgodnie z art. 10 rozporządzenia (UE, Euratom) 2023/2841 (IICB). Przy opracowywaniu informacji o dostępności usług ENISA konsultuje się również z odpowiednimi zainteresowanymi stronami z sektora cyberbezpieczeństwa, w tym z dostawcami usług zarządzanych w zakresie bezpieczeństwa. ENISA przygotowuje podobne zestawienie, po poinformowaniu Rady i konsultacji z EU-CyCLONe i Komisją oraz, w stosownych przypadkach, z Wysokim Przedstawicielem, w celu określenia potrzeb użytkowników, o których mowa w ust. 3 lit. c) niniejszego artykułu.

7. Komisja jest uprawniona do przyjmowania zgodnie z art. 23 aktów delegowanych w celu uzupełnienia niniejszego rozporządzenia poprzez szczegółowe określenie rodzajów i liczby usług reagowania wymaganych na potrzeby rezerwy cyberbezpieczeństwa UE. Przygotowując te akty delegowane, Komisja bierze pod uwagę zestawienie, o którym mowa w ust. 6 niniejszego artykułu, oraz może wymieniać porady i współpracować z grupą współpracy NIS oraz ENISA.

Artykuł 15

Wnioski o wsparcie z rezerwy cyberbezpieczeństwa UE

1. Użytkownicy, o których mowa w art. 14 ust. 3, mogą występować z wnioskami o usługi z rezerwy cyberbezpieczeństwa UE w celu wsparcia reagowania na poważne incydenty w cyberbezpieczeństwie, incydenty w cyberbezpieczeństwie na dużą skalę lub incydenty równoważne incydentom w cyberbezpieczeństwie na dużą skalę oraz wstępnego usuwania skutków takich incydentów.

2. Aby otrzymać wsparcie z rezerwy cyberbezpieczeństwa UE, użytkownicy, o których mowa w art. 14 ust. 3, podejmują wszelkie odpowiednie środki łagodzące skutki incydentu, w odniesieniu do którego wystąpiono z wnioskiem o wsparcie, obejmujące, w stosownych przypadkach, zapewnienie bezpośredniej pomocy technicznej i innych zasobów, aby wspomóc reagowanie na incydent, oraz działania służące usunięciu skutków incydentu.

3. Wnioski o wsparcie przekazuje się instytucji zamawiającej w następujący sposób:

a) w przypadku użytkowników, o których mowa w art. 14 ust. 3 lit. a) niniejszego rozporządzenia – za pośrednictwem pojedynczego punktu kontaktowego wyznaczonego lub ustanowionego zgodnie z art. 8 ust. 3 dyrektywy (UE) 2022/2555;

b) w przypadku użytkownika, o którym mowa w art. 14 ust. 3 lit. b) – przez tego użytkownika;

c) w przypadku użytkowników, o których mowa w art. 14 ust. 3 lit. c) – za pośrednictwem pojedynczego punktu kontaktowego, o którym mowa w art. 19 ust. 9.

4. W przypadku wniosków od użytkowników, o których mowa w art. 14 ust. 3 lit. a), państwa członkowskie informują sieć CSIRT oraz, w stosownych przypadkach, EU-CyCLONe o wnioskach od swoich użytkowników o wsparcie w reagowaniu na incydenty i we wstępnym usuwaniu skutków incydentów na podstawie niniejszego artykułu.

5. Wnioski o wsparcie w reagowaniu na incydenty i we wstępnym usuwaniu skutków incydentów zawierają:

a) odpowiednie informacje na temat podmiotu, na który incydent ma wpływ, oraz potencjalnych skutków incydentu dla:

   (i) w przypadku użytkowników, o których mowa w art. 14 ust. 3 lit. a) – państw członkowskich i użytkowników, których dotyczy dany incydent, w tym ryzyka rozprzestrzenienia się incydentu na inne państwo członkowskie;

(ii) w przypadku użytkownika, o którym mowa w art. 14 ust. 3 lit. b) – instytucji, organów i jednostek organizacyjnych Unii, których to dotyczy;

(iii) w przypadku użytkowników, o których mowa w art. 14 ust. 3 lit. c) – państw trzecich stowarzyszonych z programem „Cyfrowa Europa", których to dotyczy;

b) informacje na temat usługi, której dotyczy wniosek, wraz z informacjami na temat planowanego wykorzystania wsparcia, którego dotyczy wniosek, w tym wskazanie szacowanych potrzeb;

c) odpowiednie informacje o środkach zastosowanych w celu złagodzenia skutków incydentu, w odniesieniu do którego wystąpiono z wnioskiem o wsparcie, o których mowa w ust. 2;

d) w stosownych przypadkach – dostępne informacje na temat innych form wsparcia dostępnych dla podmiotu, którego dotyczy dany incydent.

6. ENISA, we współpracy z Komisją i EU-CyCLONe, opracowuje wzór ułatwiający składanie wniosków o wsparcie z rezerwy cyberbezpieczeństwa UE.

7. Komisja może w drodze aktów wykonawczych doprecyzować szczegółowe ustalenia proceduralne dotyczące sposobu, w jaki należy składać wnioski o usługi wsparcia z rezerwy cyberbezpieczeństwa UE i sposobu, w jaki należy odpowiadać na te wnioski zgodnie z niniejszym artykułem, art. 16 ust. 1 i art. 19 ust. 10, w tym ustalenia dotyczące składania takich wniosków oraz udzielania odpowiedzi i wzorów sprawozdań, o których mowa w art. 16 ust. 9. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 24 ust. 2.

Artykuł 16

Wdrożenie wsparcia z rezerwy cyberbezpieczeństwa UE

1. W przypadku wniosków od użytkowników, o których mowa w art. 14 ust. 3 lit. a) i b), wnioski o wsparcie z rezerwy cyberbezpieczeństwa UE oceniane są przez instytucję zamawiającą. Odpowiedź przekazuje się użytkownikom, o których mowa w art. 14 ust. 3 lit. a) i b), niezwłocznie, a w każdym razie nie później niż 48 godzin od złożenia wniosku, aby zapewnić skuteczność wsparcia. Instytucja zamawiająca informuje Radę i Komisję o wynikach tego procesu.

2. W odniesieniu do informacji udostępnianych w trakcie zwracania się o usługi z rezerwy cyberbezpieczeństwa UE i świadczenia usług z tej rezerwy wszystkie strony zaangażowane w stosowanie niniejszego rozporządzenia:

a) ograniczają wykorzystywanie i udostępnianie tych informacji do tego, co jest konieczne do wypełnienia ich obowiązków lub funkcji wynikających z niniejszego rozporządzenia;

b) wykorzystują i udostępniają wszelkie informacje, które są poufne lub niejawne na podstawie prawa Unii i prawa krajowego, wyłącznie zgodnie z tym prawem; oraz

c) zapewniają skuteczną, efektywną i bezpieczną wymianę informacji, w stosownych przypadkach poprzez wykorzystanie i przestrzeganie odpowiednich protokołów udostępniania informacji, w tym kodu poufności TLP.

3. Oceniając indywidualne wnioski na podstawie art. 16 ust. 1 i art. 19 ust. 10, instytucja zamawiająca lub Komisja, stosownie do przypadku, oceniają najpierw, czy spełnione są kryteria, o których mowa w art. 15 ust. 1 i 2. Jeżeli są spełnione, oceniają one czas trwania i charakter wsparcia, które jest odpowiednie, biorąc pod uwagę cel, o którym mowa w art. 1 ust. 3 lit. b), oraz, w stosownych przypadkach, następujące kryteria:

a) skala i dotkliwość incydentu;

b) rodzaj podmiotu, na który incydent ma wpływ, przy czym jako ważniejsze traktuje się incydenty mające wpływ na podmioty kluczowe, o których mowa w art. 3 ust. 1 dyrektywy (UE) 2022/2555;

c) potencjalne skutki incydentu dla państw członkowskich, instytucji, organów lub jednostek organizacyjnych Unii lub państw trzecich stowarzyszonych z programem „Cyfrowa Europa", na które incydent ma wpływ;

d) potencjalny transgraniczny charakter incydentu oraz ryzyko rozprzestrzenienia się incydentu na inne państwa członkowskie, instytucje, organy lub jednostki organizacyjne Unii lub państwa trzecie stowarzyszone z programem „Cyfrowa Europa";

e) środki podjęte przez użytkownika w celu wsparcia reagowania oraz działania służące wstępnemu usunięciu skutków incydentu, o których mowa w art. 15 ust. 2.

4. Aby nadać wnioskom priorytety, w przypadku jednoczesnych wniosków od użytkowników, o których mowa w art. 14 ust. 3, w stosownych przypadkach uwzględnia się kryteria, o których mowa w ust. 3 niniejszego artykułu, bez uszczerbku dla zasady lojalnej współpracy między państwami członkowskimi a instytucjami, organami i jednostkami organizacyjnymi Unii. W przypadku gdy co najmniej dwa wnioski zostaną ocenione jako równorzędne na podstawie tych kryteriów, wyższy priorytet nadaje się wnioskom od użytkowników z państw członkowskich. W przypadku gdy obsługę rezerwy cyberbezpieczeństwa UE i zarządzanie nią powierzono, w całości lub w części, ENISA zgodnie z art. 14 ust. 5, ENISA i Komisja ściśle współpracują w celu uszeregowania wniosków według priorytetów zgodnie z niniejszym ustępem.

5. Usługi z rezerwy cyberbezpieczeństwa UE świadczone są zgodnie ze szczegółowymi umowami między zaufanym dostawcą usług zarządzanych w zakresie bezpieczeństwa a użytkownikiem, któremu udziela się wsparcia w ramach rezerwy cyberbezpieczeństwa UE. Usługi te mogą być świadczone zgodnie ze szczegółowymi umowami między zaufanym dostawcą usług zarządzanych w zakresie bezpieczeństwa, użytkownikiem i podmiotem, którego dotyczy incydent. Wszystkie umowy, o których mowa w niniejszym ustępie, zawierają między innymi warunki dotyczące odpowiedzialności.

6. Umowy, o których mowa w ust. 5, opierają się na wzorach przygotowanych przez ENISA po konsultacji z państwami członkowskimi oraz, w stosownych przypadkach, innymi użytkownikami rezerwy cyberbezpieczeństwa UE.

7. Komisja, ENISA i użytkownicy rezerwy cyberbezpieczeństwa UE nie ponoszą odpowiedzialności umownej za szkody wyrządzone osobom trzecim przez usługi świadczone w ramach wdrażania rezerwy cyberbezpieczeństwa UE.

8. Użytkownicy mogą korzystać z usług rezerwy cyberbezpieczeństwa UE świadczonych w odpowiedzi na wniosek złożony na podstawie art. 15 ust. 1 wyłącznie w celu wsparcia reagowania na poważne incydenty w cyberbezpieczeństwie, incydenty w cyberbezpieczeństwie na dużą skalę lub incydenty równoważne incydentom w cyberbezpieczeństwie na dużą skalę oraz wstępnego usuwania skutków takich incydentów. Mogą oni korzystać z tych usług wyłącznie w odniesieniu do:

a) podmiotów działających w sektorach kluczowych lub podmiotów działających w innych sektorach krytycznych, w przypadku użytkowników, o których mowa w art. 14 ust. 3 lit. a), oraz równoważnych podmiotów w przypadku użytkowników, o których mowa w art. 14 ust. 3 lit. c); oraz

b) instytucji, organów i jednostek organizacyjnych Unii, w przypadku użytkowników, o których mowa w art. 14 ust. 3 lit. b).

9. W terminie dwóch miesięcy od zakończenia wsparcia użytkownicy, którzy otrzymali wsparcie, przekazują sprawozdanie podsumowujące na temat świadczonej usługi, osiągniętych wyników i zdobytych doświadczeń:

a) Komisji, ENISA, sieci CSIRT i EU-CyCLONe – w przypadku użytkowników, o których mowa w art. 14 ust. 3 lit. a);

b) Komisji, ENISA i IICB – w przypadku użytkownika, o którym mowa w art. 14 ust. 3 lit. b);

c) Komisji – w przypadku użytkowników, o których mowa w art. 14 ust. 3 lit. c).

Komisja przekazuje każde sprawozdanie otrzymane od użytkowników, o których mowa w art. 14 ust. 3, zgodnie z akapitem pierwszym lit. c) niniejszego ustępu, Radzie i Wysokiemu Przedstawicielowi.

10. W przypadku gdy obsługę rezerwy cyberbezpieczeństwa UE i zarządzanie nią powierzono, w całości lub w części, ENISA zgodnie z art. 14 ust. 5 niniejszego rozporządzenia, ENISA regularnie składa sprawozdania Komisji i konsultuje się z nią w tym zakresie. W tym kontekście ENISA natychmiast przesyła Komisji wszelkie wnioski otrzymane od użytkowników, o których mowa w art. 14 ust. 3 lit. c) niniejszego rozporządzenia, oraz, w przypadku gdy jest to wymagane do celów ustalenia priorytetów na podstawie niniejszego artykułu, wszelkie wnioski, które otrzymała od użytkowników, o których mowa w art. 14 ust. 3 lit. a) lub b) niniejszego rozporządzenia. Obowiązki określone w niniejszym ustępie pozostają bez uszczerbku dla art. 14 rozporządzenia (UE) 2019/881.

11. W przypadku użytkowników, o których mowa w art. 14 ust. 3 lit. a) i b), instytucja zamawiająca regularnie i co najmniej dwa razy w roku składa grupie współpracy NIS sprawozdania na temat wykorzystania i wyników wsparcia.

12. W przypadku użytkowników, o których mowa w art. 14 ust. 3 lit. c), Komisja składa sprawozdania Radzie oraz regularnie i co najmniej dwa razy w roku informuje Wysokiego Przedstawiciela o wykorzystaniu i wynikach wsparcia.

Artykuł 17

Zaufani dostawcy usług zarządzanych w zakresie bezpieczeństwa

1. W postępowaniach o udzielenie zamówienia do celów utworzenia rezerwy cyberbezpieczeństwa UE instytucja zamawiająca działa zgodnie z zasadami określonymi w rozporządzeniu (UE, Euratom) 2024/2509 oraz zgodnie z następującymi zasadami:

a) zapewnienie, aby usługi w ramach rezerwy cyberbezpieczeństwa UE, traktowane jako całość, obejmowały usługi, które mogą być wprowadzone we wszystkich państwach członkowskich, z uwzględnieniem w szczególności krajowych wymogów dotyczących świadczenia takich usług, w tym języków, certyfikacji lub akredytacji;

b) zapewnienie ochrony podstawowych interesów Unii i jej państw członkowskich w zakresie bezpieczeństwa;

c) zapewnienie, aby rezerwa cyberbezpieczeństwa UE wnosiła unijną wartość dodaną poprzez wkład w osiągnięcie celów określonych w art. 3 rozporządzenia (UE) 2021/694, w tym promowanie rozwoju umiejętności w dziedzinie cyberbezpieczeństwa w Unii.

2. Przy zamawianiu usług na potrzeby rezerwy cyberbezpieczeństwa UE instytucja zamawiająca uwzględnia w dokumentach zamówienia następujące kryteria i wymogi:

a) dostawca musi wykazać, że jego personel charakteryzuje się najwyższym stopniem uczciwości zawodowej, niezależności, odpowiedzialności i kompetencji technicznych niezbędnych do wykonywania działań w danej dziedzinie oraz zapewnia trwałość i ciągłość wiedzy fachowej, a także wymagane zasoby techniczne;

b) dostawca oraz wszelkie odpowiednie jednostki zależne i podwykonawcy muszą przestrzegać mających zastosowanie przepisów dotyczących ochrony informacji niejawnych oraz dysponować odpowiednimi środkami, w tym, w stosownych przypadkach, wzajemnymi umowami, w celu ochrony informacji poufnych dotyczących usług, a w szczególności dowodów, ustaleń i sprawozdań;

c) dostawca musi dostarczyć wystarczające dowody na to, że jego struktura zarządzania jest przejrzysta, nie zagraża jego bezstronności i jakości świadczonych przez niego usług ani nie powoduje konfliktów interesów;

d) dostawca musi posiadać odpowiednie poświadczenie bezpieczeństwa, przynajmniej w odniesieniu do personelu mającego wprowadzać usługi, jeżeli wymaga tego państwo członkowskie;

e) dostawca musi dysponować odpowiednim poziomem bezpieczeństwa swoich systemów informatycznych;

f) dostawca musi być wyposażony w sprzęt i oprogramowanie niezbędne do obsługi żądanej usługi, które nie zawiera znanych możliwych do wykorzystania podatności, obejmuje najnowsze aktualizacje zabezpieczeń i w każdym przypadku jest zgodne z wszelkimi mającymi zastosowanie przepisami rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/2847 ([23]);

g) dostawca musi być w stanie wykazać, że ma doświadczenie w świadczeniu podobnych usług odpowiednim organom krajowym lub podmiotom działającym w sektorach kluczowych lub podmiotom działającym w innych sektorach krytycznych;

h) dostawca musi być w stanie zapewnić usługę w krótkim terminie w państwach członkowskich, w których może świadczyć tę usługę;

i) dostawca musi być w stanie zapewnić usługę w co najmniej jednym języku urzędowym instytucji Unii lub państwa członkowskiego, zgodnie z wszelkimi wymogami państw członkowskich lub użytkowników, o których mowa w art. 14 ust. 3 lit. b) i c), w których dostawca może świadczyć tę usługę;

j) po wprowadzeniu europejskiego programu certyfikacji cyberbezpieczeństwa usług zarządzanych w zakresie bezpieczeństwa zgodnie z rozporządzeniem (UE) 2019/881 dostawca musi być certyfikowany zgodnie z tym programem w okresie 2 lat od dnia rozpoczęcia stosowania programu;

([23]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) nr 168/2013 i (UE) 2019/1020 i dyrektywy (UE) 2020/1828 (akt o cyberodporności) (Dz.U. L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

k) dostawca musi uwzględniać w ofercie przetargowej warunki przekształcenia wszelkich niewykorzystanych usług reagowania na incydenty, które mogłyby zostać przekształcone w usługi w zakresie gotowości ściśle związane z reagowaniem na incydenty, takie jak ćwiczenia lub szkolenia.

3. Do celów zamawiania usług na potrzeby rezerwy cyberbezpieczeństwa UE instytucja zamawiająca może, w stosownych przypadkach, opracować dodatkowe kryteria i wymogi oprócz kryteriów, o których mowa w ust. 2, w ścisłej współpracy z państwami członkowskimi.

Artykuł 18

Działania w zakresie wspierania wzajemnej pomocy

1. Mechanizm cyberkryzysowy zapewnia wsparcie pomocy technicznej udzielanej przez jedno państwo członkowskie drugiemu państwu członkowskiemu dotkniętemu poważnym incydentem w cyberbezpieczeństwie lub incydentem w cyberbezpieczeństwie na dużą skalę, w tym w przypadkach, o których mowa w art. 11 ust. 3 lit. f) dyrektywy (UE) 2022/2555.

2. Wsparcia wzajemnej pomocy technicznej, o której mowa w ust. 1 niniejszego artykułu, udziela się w formie dotacji oraz na warunkach przewidzianych w odpowiednich programach prac, o których mowa w art. 24 rozporządzenia (UE) 2021/694.

Artykuł 19

Wsparcie dla państw trzecich stowarzyszonych z programem „Cyfrowa Europa"

1. Państwo trzecie stowarzyszone z programem „Cyfrowa Europa" może wystąpić z wnioskiem o wsparcie z rezerwy cyberbezpieczeństwa UE, w przypadku gdy umowa, za pośrednictwem której jest ono stowarzyszone z programem „Cyfrowa Europa", przewiduje uczestnictwo w rezerwie cyberbezpieczeństwa UE. Umowa ta musi zawierać postanowienia zobowiązujące dane państwo trzecie stowarzyszone z programem „Cyfrowa Europa" do wypełnienia obowiązków określonych w ust. 2 i 9 niniejszego artykułu. Do celów uczestnictwa państwa trzeciego w rezerwie cyberbezpieczeństwa UE częściowe stowarzyszenie państwa trzeciego z programem „Cyfrowa Europa" może obejmować stowarzyszenie ograniczone do celu operacyjnego, o którym mowa w art. 6 ust. 1 lit. g) rozporządzenia (UE) 2021/694.

2. W terminie trzech miesięcy od zawarcia umowy, o której mowa w ust. 1, a w każdym przypadku przed otrzymaniem jakiegokolwiek wsparcia z rezerwy cyberbezpieczeństwa UE państwo trzecie stowarzyszone z programem „Cyfrowa Europa" przekazuje Komisji informacje na temat swoich zdolności w zakresie cyberodporności i zarządzania ryzykiem, w tym co najmniej informacje na temat środków krajowych wprowadzonych w celu przygotowania się na poważne incydenty w cyberbezpieczeństwie, incydenty w cyberbezpieczeństwie na dużą skalę lub incydenty równoważne incydentom w cyberbezpieczeństwie na dużą skalę, a także informacje na temat odpowiedzialnych podmiotów krajowych, w tym zespołów reagowania na komputerowe incydenty w bezpieczeństwie lub równoważnych podmiotów, ich zdolności i przydzielonych im zasobów. Państwo trzecie stowarzyszone z programem „Cyfrowa Europa" regularnie i co najmniej raz w roku przekazuje aktualizacje tych informacji. Komisja przekazuje te informacje Wysokiemu Przedstawicielowi i ENISA do celów ułatwienia stosowania ust. 11.

3. Komisja regularnie i co najmniej raz w roku ocenia następujące kryteria w odniesieniu do każdego państwa trzeciego stowarzyszonego z programem „Cyfrowa Europa", o którym mowa w ust. 1:

a) czy państwo to przestrzega warunków umowy, o której mowa w ust. 1, w zakresie, w jakim warunki te odnoszą się do uczestnictwa w rezerwie cyberbezpieczeństwa UE;

b) czy państwo to podjęło odpowiednie kroki w celu przygotowania się na poważne incydenty w cyberbezpieczeństwie lub incydenty równoważne incydentom w cyberbezpieczeństwie na dużą skalę, w oparciu o informacje, o których mowa w ust. 2; oraz

c) czy udzielenie wsparcia jest spójne z polityką Unii wobec tego państwa i ogólnymi stosunkami z tym państwem oraz czy jest spójne z innymi politykami Unii w dziedzinie bezpieczeństwa.

Przeprowadzając ocenę, o której mowa w akapicie pierwszym, Komisja konsultuje się z Wysokim Przedstawicielem w odniesieniu do kryterium, o którym mowa w lit. c) tego akapitu.

W przypadku gdy Komisja stwierdzi, że państwo trzecie stowarzyszone z programem „Cyfrowa Europa" spełnia wszystkie warunki, o których mowa w akapicie pierwszym, Komisja przedkłada Radzie wniosek o przyjęcie aktu wykonawczego zgodnie z ust. 4 w celu zezwolenia na udzielenie temu państwu wsparcia z rezerwy cyberbezpieczeństwa UE.

4. Rada może przyjąć akty wykonawcze, o których mowa w ust. 3. Te akty wykonawcze stosuje się nie dłużej niż przez rok. Ich obowiązywanie może zostać przedłużone. Mogą one określać maksymalną liczbę dni, przez które wsparcie może być udzielane w odpowiedzi na pojedynczy wniosek, nie mniejszą niż 75.

Do celów niniejszego artykułu Rada działa szybko i co do zasady przyjmuje akty wykonawcze, o których mowa w niniejszym ustępie, w terminie 8 tygodni od przyjęcia odpowiedniego wniosku Komisji zgodnie z ust. 3 akapit pierwszy.

5. Rada może w dowolnym momencie zmienić lub uchylić akt wykonawczy przyjęty zgodnie z ust. 4, działając na wniosek Komisji.

W przypadku gdy Rada uzna, że nastąpiła istotna zmiana dotycząca kryterium, o którym mowa w ust. 3 akapit pierwszy lit. c), może ona zmienić lub uchylić akt wykonawczy przyjęty zgodnie z ust. 4, działając z należycie uzasadnionej inicjatywy co najmniej jednego państwa członkowskiego.

6. Wykonując swoje uprawnienia wykonawcze na podstawie niniejszego artykułu, Rada stosuje kryteria, o których mowa w ust. 3 akapit pierwszy, oraz wyjaśnia swoją ocenę tych kryteriów. W szczególności, w przypadku gdy Rada działa z własnej inicjatywy zgodnie z ust. 5 akapit drugi, wyjaśnia ona istotną zmianę, o której mowa w tym akapicie.

7. Wsparcie z rezerwy cyberbezpieczeństwa UE dla państwa trzeciego stowarzyszonego z programem „Cyfrowa Europa" musi być zgodne z wszelkimi szczegółowymi warunkami określonymi w umowie, o której mowa w ust. 1.

8. Do użytkowników z państw trzecich stowarzyszonych z programem „Cyfrowa Europa" kwalifikujących się do otrzymania usług z rezerwy cyberbezpieczeństwa UE należą właściwe organy, takie jak zespoły reagowania na incydenty bezpieczeństwa komputerowego lub podmioty równoważne oraz organy ds. zarządzania kryzysowego w cyberbezpieczeństwie.

9. Każde państwo trzecie stowarzyszone z programem „Cyfrowa Europa" kwalifikujące się do wsparcia z rezerwy cyberbezpieczeństwa UE wyznacza organ, który będzie pełnił funkcję pojedynczego punktu kontaktowego do celów niniejszego rozporządzenia.

10. Wnioski o wsparcie z rezerwy cyberbezpieczeństwa UE na podstawie niniejszego artykułu oceniane są przez Komisję. Instytucja zamawiająca może udzielić wsparcia państwu trzeciemu wyłącznie w przypadku gdy i tak długo, jak obowiązuje akt wykonawczy Rady zezwalający na takie wsparcie w odniesieniu do tego państwa, przyjęty zgodnie z ust. 4 niniejszego artykułu. Odpowiedź przekazuje się użytkownikom, o których mowa w art. 14 ust. 3 lit. c), bez zbędnej zwłoki.

11. Po otrzymaniu wniosku o wsparcie na podstawie niniejszego artykułu Komisja natychmiast informuje o tym Radę. Komisja na bieżąco informuje Radę o ocenie wniosku. Komisja współpracuje również z Wysokim Przedstawicielem w odniesieniu do otrzymanych wniosków i wdrażania wsparcia przyznanego państwom trzecim stowarzyszonym z programem „Cyfrowa Europa" z rezerwy cyberbezpieczeństwa UE. Ponadto Komisja uwzględnia również wszelkie opinie przedstawione przez ENISA w odniesieniu do tych wniosków.

Artykuł 20

Koordynacja z unijnymi mechanizmami zarządzania kryzysowego

1. W przypadku gdy poważny incydent w cyberbezpieczeństwie, incydent w cyberbezpieczeństwie na dużą skalę lub incydent równoważny incydentowi w cyberbezpieczeństwie na dużą skalę wynika z klęski lub katastrofy zdefiniowanej w art. 4 pkt 1 decyzji nr 1313/2013/UE lub skutkuje taką klęską lub katastrofą, wsparcie udzielane na podstawie niniejszego rozporządzenia na potrzeby reagowania na taki incydent uzupełnia działania podejmowane na podstawie tej decyzji oraz pozostaje bez uszczerbku dla tej decyzji.

2. W przypadku incydentu w cyberbezpieczeństwie na dużą skalę lub incydentu równoważnego incydentowi w cyberbezpieczeństwie na dużą skalę, gdy uruchomione zostaną zintegrowane uzgodnienia UE dotyczące reagowania na szczeblu politycznym w sytuacjach kryzysowych na podstawie decyzji wykonawczej (UE) 2018/1993 (zwane dalej „uzgodnieniami IPCR"), wsparcie udzielane na podstawie niniejszego rozporządzenia na potrzeby reagowania na taki incydent odbywa się zgodnie z odpowiednimi procedurami w ramach uzgodnień IPCR.

ROZDZIAŁ IV

EUROPEJSKI MECHANIZM PRZEGLĄDU INCYDENTÓW W CYBERBEZPIECZEŃSTWIE

Artykuł 21

Europejski mechanizm przeglądu incydentów w cyberbezpieczeństwie

1. Na wniosek Komisji lub EU-CyCLONe ENISA, przy wsparciu sieci CSIRT oraz za zgodą zainteresowanych państw członkowskich, dokonuje przeglądu i oceny cyberzagrożeń, znanych możliwych do wykorzystania podatności i działań łagodzących w odniesieniu do konkretnego poważnego incydentu w cyberbezpieczeństwie lub incydentu w cyberbezpieczeństwie na dużą skalę. Po zakończeniu przeglądu i oceny incydentu oraz w celu wyciągnięcia wniosków ze zdobytych doświadczeń, aby uniknąć przyszłych incydentów lub złagodzić ich skutki, ENISA przekazuje EU-CyCLONe, sieci CSIRT, zainteresowanym państwom członkowskim i Komisji sprawozdanie z przeglądu incydentu, aby wesprzeć je w wykonywaniu ich zadań, w szczególności zadań określonych w art. 15 i 16 dyrektywy (UE) 2022/2555. W przypadku gdy incydent ma wpływ na państwo trzecie stowarzyszone z programem „Cyfrowa Europa", ENISA przekazuje sprawozdanie Radzie. W takich przypadkach Komisja przekazuje to sprawozdanie Wysokiemu Przedstawicielowi.

2. W celu przygotowania sprawozdania z przeglądu incydentu, o którym mowa w ust. 1 niniejszego artykułu, ENISA współpracuje ze wszystkimi odpowiednimi zainteresowanymi stronami, w tym przedstawicielami państw członkowskich, Komisji, innych odpowiednich instytucji, organów i jednostek organizacyjnych Unii, przemysłu, w tym dostawców usług zarządzanych w zakresie bezpieczeństwa i użytkowników usług w zakresie cyberbezpieczeństwa, oraz zbiera informacje zwrotne od nich. W stosownych przypadkach ENISA, we współpracy z CSIRT oraz, w stosownych przypadkach, z właściwymi organami wyznaczonymi lub ustanowionymi zgodnie z art. 8 ust. 1 dyrektywy (UE) 2022/2555, współpracuje również z podmiotami dotkniętymi poważnymi incydentami w cyberbezpieczeństwie lub incydentami w cyberbezpieczeństwie na dużą skalę. Przedstawiciele, z którymi przeprowadza się konsultacje, ujawniają wszelkie potencjalne konflikty interesów.

3. Sprawozdanie z przeglądu incydentu, o którym mowa w ust. 1 niniejszego artykułu, obejmuje przegląd i analizę konkretnego poważnego incydentu w cyberbezpieczeństwie lub incydentu w cyberbezpieczeństwie na dużą skalę, w tym głównych przyczyn, znanych możliwych do wykorzystania podatności i zdobytych doświadczeń. ENISA zapewnia zgodność sprawozdania z prawem unijnym lub krajowym dotyczącym ochrony informacji szczególnie chronionych lub niejawnych. Na wniosek odpowiednich państw członkowskich lub innych użytkowników, o których mowa w art. 14 ust. 3, dotkniętych incydentem, dane i informacje zawarte w sprawozdaniu obejmują wyłącznie dane zanonimizowane. Nie ujawnia się w nim jakichkolwiek szczegółów na temat aktywnie wykorzystywanych podatności, którym nie udało się jeszcze zaradzić.

4. W stosownych przypadkach sprawozdanie z przeglądu incydentu zawiera zalecenia mające na celu poprawę pozycji Unii w kwestiach cyberprzestrzeni oraz może obejmować najlepsze praktyki i wnioski wyciągnięte z doświadczeń zdobytych przez odpowiednie zainteresowane strony.

5. ENISA może wydać publicznie dostępną wersję sprawozdania z przeglądu incydentu. Ta wersja sprawozdania zawiera wyłącznie wiarygodne informacje publiczne lub inne wiarygodne informacje za zgodą zainteresowanych państw członkowskich oraz, w odniesieniu do informacji dotyczących użytkownika, o którym mowa w art. 14 ust. 3 lit. b) lub c) – za zgodą tego użytkownika.

ROZDZIAŁ V

PRZEPISY KOŃCOWE

Artykuł 22

Zmiany w rozporządzeniu (UE) 2021/694

W rozporządzeniu (UE) 2021/694 wprowadza się następujące zmiany:

1) w art. 6 wprowadza się następujące zmiany:

a) w ust. 1 wprowadza się następujące zmiany:

(i) dodaje się lit. aa) w brzmieniu:

„aa) wspieraniu rozwoju europejskiego systemu ostrzeżeń dotyczących cyberbezpieczeństwa ustanowionego na podstawie art. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2025/38 (zwanego dalej »europejskim systemem ostrzeżeń dotyczących cyberbezpieczeństwa«) (*), w tym rozwijaniu, wprowadzaniu i eksploatacji krajowych centrów cyberbezpieczeństwa i transgranicznych centrów cyberbezpieczeństwa, które wnoszą wkład w orientację sytuacyjną w Unii oraz w zwiększanie unijnych zdolności wywiadowczych w zakresie cyberzagrożeń;

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2025/38 z dnia 19 grudnia 2024 r. w sprawie ustanowienia środków mających na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania cyberzagrożeń i incydentów oraz przygotowywania się i reagowania na takie zagrożenia i incydenty oraz w sprawie zmiany rozporządzenia (UE) 2021/694 (akt w sprawie cybersolidarności) (Dz. U. L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).";

(ii) dodaje się literę w brzmieniu:

„g) utworzeniu i obsłudze mechanizmu cyberkryzysowego ustanowionego na podstawie art. 10 rozporządzenia (UE) 2025/38, w tym rezerwy cyberbezpieczeństwa UE ustanowionej na podstawie art. 14 tego rozporządzenia (zwanej dalej »rezerwą cyberbezpieczeństwa UE«), w celu wspierania państw członkowskich w przygotowaniu się na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę oraz reagowaniu na nie, stanowiącego uzupełnienie krajowych zasobów i zdolności oraz innych form wsparcia dostępnych na poziomie Unii, oraz w celu wspierania innych użytkowników w reagowaniu poważne incydenty w cyberbezpieczeństwie i incydenty równoważne incydentom w cyberbezpieczeństwie na dużą skalę.";

b) ust. 2 otrzymuje brzmienie:

„2. Działania w ramach celu szczegółowego nr 3 realizowane są przede wszystkim za pośrednictwem Europejskiego Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa oraz sieci krajowych ośrodków koordynacji zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2021/887 (*). Jednakże, rezerwa cyberbezpieczeństwa UE jest wdrażania przez Komisję oraz, zgodnie z art. 14 ust. 6 rozporządzenia (UE) 2025/38, przez ENISA.

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/887 z dnia 20 maja 2021 r. ustanawiające Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa oraz sieć krajowych ośrodków koordynacji (Dz.U. L 202 z 8.6.2021, s. 1).";

2) w art. 9 wprowadza się następujące zmiany:

a) ust. 2 lit. b), c) i d) otrzymują brzmienie:

„b) 1 760 806 000 EUR na cel szczegółowy nr 2 – Sztuczna inteligencja;

c) 1 372 020 000 EUR na cel szczegółowy nr 3 – Cyberbezpieczeństwo i zaufanie;

d) 482 640 000 EUR na cel szczegółowy nr 4 – Zaawansowane umiejętności cyfrowe;";

b) dodaje się ustęp w brzmieniu:

„8. Na zasadzie odstępstwa od art. 12 ust. 1 rozporządzenia finansowego niewykorzystane środki na zobowiązania i środki na płatności przeznaczone na działania dotyczące wdrażania rezerwy cyberbezpieczeństwa UE oraz działania w zakresie wspierania wzajemnej pomocy na podstawie rozporządzenia (UE) 2025/38 służące osiągnięciu celów określonych w art. 6 ust. 1 lit. g) niniejszego rozporządzenia są automatycznie przenoszone i mogą być przeznaczane na zobowiązania i płatności realizowane do dnia 31 grudnia następnego roku budżetowego. Parlament Europejski i Rada są informowane o środkach przeniesionych zgodnie z art. 12 ust. 6 rozporządzenia finansowego.";

3) w art. 12 wprowadza się następujące zmiany:

a) dodaje się ustępy w brzmieniu:

„5a. Ustęp 5 nie ma zastosowania – w zakresie, w jakim dotyczy podmiotów prawnych, które mają siedzibę w Unii, ale są kontrolowane z państw trzecich – do wszelkich działań wdrażających europejski system ostrzeżeń dotyczących cyberbezpieczeństwa w przypadku gdy w odniesieniu do danego działania spełnione są oba poniższe warunki:

a) istnieje realne ryzyko, biorąc pod uwagę wyniki zestawienia sporządzonego zgodnie z art. 9 ust. 4 rozporządzenia (UE) 2025/38 , że niezbędne narzędzia, infrastruktura lub usługi wystarczające do tego, aby działanie to odpowiednio przyczyniło się do osiągnięcia celu, jakim jest europejski system ostrzeżeń dotyczących cyberbezpieczeństwa, nie będą dostępne ze strony podmiotów prawnych mających siedzibę lub uznanych za mające siedzibę w państwach członkowskich i kontrolowanych przez państwa członkowskie lub obywateli państw członkowskich;

b) ryzyko dla bezpieczeństwa związane z zamówieniami od takich podmiotów prawnych w ramach europejskiego systemu ostrzeżeń dotyczących cyberbezpieczeństwa jest proporcjonalne do korzyści i nie narusza podstawowych interesów bezpieczeństwa Unii i jej państw członkowskich.

5b. Ustęp 5 nie ma zastosowania – w zakresie, w jakim dotyczy podmiotów prawnych, które mają siedzibę w Unii, ale są kontrolowane z państw trzecich – do działań wdrażających rezerwę cyberbezpieczeństwa UE w przypadku gdy w odniesieniu do danego działania spełnione są oba poniższe warunki:

a) istnieje realne ryzyko, biorąc pod uwagę wyniki zestawienia sporządzonego zgodnie z art. 14 ust. 6 rozporządzenia (UE) 2025/38, że technologia, wiedza specjalistyczna lub zdolności niezbędne i wystarczające do tego, aby rezerwa cyberbezpieczeństwa UE mogła odpowiednio wykonywać swoje funkcje, nie będą dostępne ze strony podmiotów prawnych mających siedzibę lub uznanych za mające siedzibę w państwach członkowskich i kontrolowanych przez państwa członkowskie lub obywateli państw członkowskich;

b) ryzyko dla bezpieczeństwa związane z włączeniem takich podmiotów prawnych do rezerwy cyberbezpieczeństwa UE jest proporcjonalne do korzyści i nie narusza podstawowych interesów bezpieczeństwa Unii i jej państw członkowskich.";

b) ust. 6 otrzymuje brzmienie:

„6. Jeśli istnieją należycie uzasadnione względy bezpieczeństwa, w programie prac można również przewidzieć, że podmioty prawne z siedzibą w państwach stowarzyszonych i podmioty prawne z siedzibą w Unii, lecz kontrolowane z państwa trzeciego, mogą kwalifikować się do uczestnictwa we wszystkich lub niektórych działaniach w ramach celów szczegółowych nr 1 i 2 tylko wówczas, jeżeli spełniają wymogi, które te podmioty prawne powinny spełniać, aby zagwarantować ochronę podstawowych interesów Unii i jej państw członkowskich w zakresie bezpieczeństwa oraz zapewnić ochronę informacji zawartych w dokumentach niejawnych. Wymogi te określa się w programie prac.

Akapit pierwszy ma także zastosowanie – w zakresie, w jakim dotyczy podmiotów prawnych, które mają siedzibę w Unii, ale są kontrolowane z państw trzecich – do działań w ramach celu szczegółowego nr 3:

a) wdrażania europejskiego systemu ostrzeżeń dotyczących cyberbezpieczeństwa w przypadku gdy zastosowanie ma ust. 5a; oraz

b) wdrażania rezerwy cyberbezpieczeństwa UE w przypadku gdy zastosowanie ma ust. 5b.";

4) art. 14 ust. 2 otrzymuje brzmienie:

„2. Program może zapewniać finansowanie w dowolnej formie przewidzianej w rozporządzeniu finansowym, w tym w szczególności poprzez zamówienia stanowiące podstawową formę lub poprzez dotacje i nagrody.

W przypadku gdy osiągnięcie celu działania wymaga zamówienia innowacyjnych towarów i usług, dotacje można przyznać tylko beneficjentom będącym instytucjami zamawiającymi lub podmiotami zamawiającymi zdefiniowanymi w dyrektywach Parlamentu Europejskiego i Rady 2014/24/UE (*) i 2014/25/UE (**).

W przypadku gdy do osiągnięcia celów działania niezbędne jest dostarczenie innowacyjnych towarów lub usług, które nie są jeszcze powszechnie dostępne na rynku, instytucja zamawiająca lub podmiot zamawiający mogą zezwolić na udzielenie więcej niż jednego zamówienia w ramach tego samego postępowania o udzielenie zamówienia.

Z powodów należycie uzasadnionych względami bezpieczeństwa publicznego instytucja zamawiająca lub podmiot zamawiający mogą wymagać, aby miejsce wykonania zamówienia znajdowało się na terytorium Unii.

Realizując postępowania o udzielenie zamówienia na potrzeby rezerwy cyberbezpieczeństwa UE, Komisja i ENISA mogą działać jako centralna jednostka zakupująca w celu udzielania zamówień w imieniu lub na rzecz państw trzecich stowarzyszonych z Programem zgodnie z art. 10 niniejszego rozporządzenia. Komisja i ENISA mogą również działać jako hurtownik, kupując, przechowując i odsprzedając lub przekazując jako darowiznę towary i usługi, w tym

przedmioty najmu, tym państwom trzecim. Na zasadzie odstępstwa od art. 168 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) 2024/2509 (***) wniosek jednego państwa trzeciego wystarcza, aby upoważnić Komisję lub ENISA do działania.

Realizując postępowania o udzielenie zamówienia na potrzeby rezerwy cyberbezpieczeństwa UE, Komisja i ENISA mogą działać jako centralna jednostka zakupująca w celu udzielania zamówień w imieniu lub na rzecz instytucji, organów lub jednostek organizacyjnych Unii. Komisja i ENISA mogą również działać jako hurtownik, kupując, przechowując i odsprzedając lub przekazując jako darowiznę towary i usługi, w tym przedmioty najmu, instytucjom, organom lub jednostkom organizacyjnym Unii. Na zasadzie odstępstwa od art. 168 ust. 3 rozporządzenia (UE, Euratom) 2024/2509 wniosek jednej instytucji, jednego organu lub jednej jednostki organizacyjnej Unii wystarcza, aby upoważnić Komisję lub ENISA do działania.

Program może również zapewniać finansowanie w formie instrumentów finansowych w operacjach łączonych.

(*) Dyrektywa Parlamentu Europejskiego i Rady 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zamówień publicznych, uchylająca dyrektywę 2004/18/WE (Dz.U. L 94 z 28.3.2014, s. 65).
(**) Dyrektywa Parlamentu Europejskiego i Rady 2014/25/UE z dnia 26 lutego 2014 r. w sprawie udzielania zamówień przez podmioty działające w sektorach gospodarki wodnej, energetyki, transportu i usług pocztowych, uchylająca dyrektywę 2004/17/WE (Dz.U. L 94 z 28.3.2014, s. 243).
(***) Rozporządzenie Parlamentu Europejskiego (UE, Euratom) 2024/2509 z dnia 23 września 2024 r. w sprawie zasad finansowych mających zastosowanie do budżetu ogólnego Unii (Dz.U. L, 2024/2509, 26.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).";

5) dodaje się artykuł w brzmieniu:

„*Artykuł 16a*

Konflikt przepisów

W przypadku działań służących wdrażaniu europejskiego systemu ostrzeżeń dotyczących cyberbezpieczeństwa przepisami mającymi zastosowanie są przepisy art. 4, 5 i 9 rozporządzenia (UE) 2025/38. W przypadku konfliktu między przepisami niniejszego rozporządzenia a art. 4, 5 i 9 rozporządzenia (UE) 2025/38 te ostatnie mają pierwszeństwo i mają zastosowanie do tych konkretnych działań.

W przypadku rezerwy cyberbezpieczeństwa UE szczegółowe zasady uczestnictwa państw trzecich stowarzyszonych z programem określono w art. 19 rozporządzenia (UE) 2025/38. W przypadku konfliktu między przepisami niniejszego rozporządzenia a art. 19 rozporządzenia (UE) 2025/38 ten ostatni ma pierwszeństwo i mają zastosowanie do tych konkretnych działań.";

6) art. 19 otrzymuje brzmienie:

„*Artykuł 19*

Dotacje

Dotacje w ramach Programu przyznaje się i zarządza się nimi zgodnie z tytułem VIII rozporządzenia finansowego i mogą one pokrywać do 100 % kosztów kwalifikowalnych, bez uszczerbku dla zasady współfinansowania ustanowionej w art. 190 rozporządzenia finansowego. Takie dotacje przyznaje się i zarządza się nimi w sposób określony dla poszczególnych celów.

Wsparcie w formie dotacji może przyznawać bezpośrednio ECCC bez zaproszenia do składania wniosków państwom członkowskim wybranym zgodnie z art. 9 rozporządzenia (UE) 2025/38, oraz konsorcjum przyjmującemu, o którym mowa w art. 5 rozporządzenia (UE) 2025/38, zgodnie z art. 195 ust. 1 lit. d) rozporządzenia finansowego.

Wsparcie w formie dotacji do celów mechanizmu cyberkryzysowego może przyznawać bezpośrednio ECCC państwom członkowskim bez zaproszenia do składania wniosków, zgodnie z art. 195 ust. 1 lit. d) rozporządzenia finansowego.

W odniesieniu do działań w zakresie wspierania wzajemnej pomocy przewidzianych w art. 18 rozporządzenia (UE) 2025/38 ECCC informuje Komisję i ENISA o wnioskach państw członkowskich o udzielenie dotacji bezpośrednich bez zaproszenia do składania wniosków.

W odniesieniu do działań w zakresie wspierania wzajemnej pomocy przewidzianych w art. 18 rozporządzenia (UE) 2025/38, oraz zgodnie z art. 193 ust. 2 akapit drugi lit. a) rozporządzenia finansowego w należycie uzasadnionych przypadkach koszty można uznać za kwalifikowalne, nawet jeżeli zostały poniesione przed przedłożeniem wniosku o udzielenie dotacji.";

7) w załącznikach I i II wprowadza się zmiany zgodnie z załącznikiem do niniejszego rozporządzenia.

Artykuł 23

Wykonywanie przekazanych uprawnień

1. Powierzenie Komisji uprawnień do przyjmowania aktów delegowanych podlega warunkom określonym w niniejszym artykule.

2. Uprawnienia do przyjmowania aktów delegowanych, o których mowa w art. 14 ust. 7, powierza się Komisji na okres 5 lat od dnia 5 lutego 2025 r. Komisja sporządza sprawozdanie dotyczące przekazania uprawnień nie później niż 9 miesięcy przed końcem okresu 5 lat. Przekazanie uprawnień zostaje automatycznie przedłużone na takie same okresy, chyba że Parlament Europejski lub Rada sprzeciwią się takiemu przedłużeniu nie później niż 3 miesiące przed końcem każdego okresu.

3. Przekazanie uprawnień, o którym mowa w art. 14 ust. 7, może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna następnego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej* lub w późniejszym terminie określonym w tej decyzji. Nie wpływa ona na ważność już obowiązujących aktów delegowanych.

4. Przed przyjęciem aktu delegowanego Komisja konsultuje się z ekspertami wyznaczonymi przez każde państwo członkowskie zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa.

5. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie.

6. Akt delegowany przyjęty na podstawie art. 14 ust. 7 wchodzi w życie tylko wówczas, gdy ani Parlament Europejski, ani Rada nie wyraziły sprzeciwu w terminie 2 miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie, lub gdy, przed upływem tego terminu, zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o 2 miesiące z inicjatywy Parlamentu Europejskiego lub Rady.

Artykuł 24

Procedura komitetowa

1. Komisję wspomaga Komitet Koordynacyjny ds. Programu „Cyfrowa Europa", o którym mowa w art. 31 ust. 1 rozporządzenia (UE) 2021/694. Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011.

2. W przypadku odesłania do niniejszego ustępu stosuje się art. 5 rozporządzenia (UE) nr 182/2011.

Artykuł 25

Ocena i przegląd

1. Do dnia 5 lutego 2027 r., a następnie przynajmniej co 4 lata Komisja przeprowadzi ocenę funkcjonowania środków przewidzianych w niniejszym rozporządzeniu oraz przedłoży sprawozdanie Parlamentowi Europejskiemu i Radzie.

2. Ocena, o której mowa w ust. 1, obejmuje w szczególności:

a) liczbę utworzonych krajowych centrów cyberbezpieczeństwa i transgranicznych centrów cyberbezpieczeństwa, zakres udostępniania informacji, w tym, w miarę możliwości, wpływ na pracę sieci CSIRT, oraz zakres, w jakim przyczyniły się one do wzmocnienia wspólnego unijnego wykrywania cyberzagrożeń i incydentów oraz orientacji sytuacyjnej w tym zakresie, a także do rozwoju najnowocześniejszych technologii; wykorzystanie środków z programu „Cyfrowa Europa" na wspólnie zamawiane narzędzia, infrastrukturę lub usługi w zakresie cyberbezpieczeństwa, a także – jeśli informacje te

są dostępne – poziom współpracy między krajowymi centrami cyberbezpieczeństwa a sektorowymi i międzysektorowymi społecznościami kluczowych i ważnych podmiotów, o których mowa w art. 3 dyrektywy (UE) 2022/2555.

b) wykorzystanie i skuteczność działań w ramach mechanizmu cyberkryzysowego wspierającego gotowość, w tym szkolenia, reagowanie na poważne incydenty w cyberbezpieczeństwie, incydenty w cyberbezpieczeństwie na dużą skalę i incydenty równoważne incydentom w cyberbezpieczeństwie na dużą skalę oraz wstępne usuwanie skutków tych incydentów, w tym wykorzystanie finansowania z programu „Cyfrowa Europa" oraz wnioski i zalecenia wynikające z wdrożenia mechanizmu cyberkryzysowego;

c) wykorzystanie i skuteczność rezerwy cyberbezpieczeństwa UE w odniesieniu do rodzaju użytkowników, w tym wykorzystanie finansowania z programu „Cyfrowa Europa", korzystanie z usług, w tym ich rodzaj, średni czas reakcji na wnioski i uruchomienia rezerwy cyberbezpieczeństwa UE, odsetek usług przekształconych w usługi w zakresie gotowości związane z zapobieganiem incydentom i reagowaniem na nie oraz wnioski i zalecenia wynikające z wdrożenia rezerwy cyberbezpieczeństwa UE;

d) wkład niniejszego rozporządzenia we wzmocnienie konkurencyjnej pozycji przemysłu i usług w Unii w całej gospodarce cyfrowej, w tym mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw, a także przedsiębiorstw typu start-up, oraz wkład w realizację ogólnego celu, jakim jest wzmocnienie umiejętności i zdolności pracowników w zakresie cyberbezpieczeństwa.

3. Na podstawie sprawozdań, o których mowa w ust. 1, Komisja w stosownych przypadkach przedkłada Parlamentowi Europejskiemu i Radzie wniosek ustawodawczy dotyczący zmiany niniejszego rozporządzenia.

Artykuł 26

Wejście w życie

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 19 grudnia 2024 r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodnicząca	*Przewodniczący*
R. METSOLA	BÓKA J.

ZAŁĄCZNIK

W rozporządzeniu (UE) 2021/694 wprowadza się następujące zmiany:

1) w załączniku I sekcja „Cel szczegółowy nr 3 – Cyberbezpieczeństwo i zaufanie" otrzymuje brzmienie:

„Cel szczegółowy nr 3 – Cyberbezpieczeństwo i zaufanie

Program ma stymulować wzmocnienie, budowę i nabywanie podstawowych zdolności w celu zabezpieczenia unijnej gospodarki cyfrowej, społeczeństwa i demokracji poprzez wzmocnienie unijnego potencjału przemysłowego i konkurencyjności w dziedzinie cyberbezpieczeństwa, a także zwiększenie zdolności sektora prywatnego i publicznego do ochrony obywateli i przedsiębiorstw przed cyberzagrożeniami, w tym poprzez wspieranie wykonywania dyrektywy (UE) 2016/1148.

Początkowe, a w stosownych przypadkach późniejsze działania w ramach niniejszego celu obejmują:

1. Wspólne inwestycje z państwami członkowskimi w zaawansowane urządzenia, infrastrukturę i know-how w dziedzinie cyberbezpieczeństwa, które są niezbędne do ochrony infrastruktury krytycznej i całego jednolitego rynku cyfrowego. Takie wspólne inwestycje mogą obejmować inwestycje w infrastrukturę kwantową i zasoby danych na potrzeby cyberbezpieczeństwa, orientację sytuacyjną w cyberprzestrzeni, w tym krajowe centra cyberbezpieczeństwa i transgraniczne centra cyberbezpieczeństwa tworzące europejski system ostrzeżeń dotyczących cyberbezpieczeństwa, a także inne narzędzia, które zostaną udostępnione sektorowi publicznemu i prywatnemu w całej Europie.

2. Zwiększanie istniejących zdolności technologicznych i łączenie w sieć ośrodków kompetencji w państwach członkowskich oraz zapewnienie, aby zdolności te odpowiadały potrzebom sektora publicznego i przemysłu, w tym w odniesieniu do produktów i usług, które wzmacniają cyberbezpieczeństwo i zaufanie w ramach jednolitego rynku cyfrowego.

3. Zapewnienie szerokiego wdrożenia skutecznych, najnowocześniejszych rozwiązań z zakresu cyberbezpieczeństwa i zaufania w państwach członkowskich. Takie wdrożenie obejmuje zwiększenie bezpieczeństwa i ochrony produktów od momentu ich zaprojektowania do ich komercjalizacji.

4. Zapewnienie wsparcia w celu wyeliminowania luki w umiejętnościach w zakresie cyberbezpieczeństwa, z uwzględnieniem równowagi płci, poprzez na przykład ujednolicenie programów dotyczących umiejętności w zakresie cyberbezpieczeństwa, dostosowanie ich do konkretnych potrzeb sektorowych oraz ułatwienie dostępu do ukierunkowanych specjalistycznych szkoleń.

5. Promowanie solidarności między państwami członkowskimi w zakresie przygotowania się i reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę poprzez transgraniczne wdrażanie usług w zakresie cyberbezpieczeństwa, w tym wspieranie udzielania wzajemnej pomocy między organami publicznymi i ustanowienie rezerwy zaufanych dostawców usług zarządzanych w zakresie bezpieczeństwa na poziomie Unii.";

2) w załączniku II sekcja „Cel szczegółowy nr 3 – Cyberbezpieczeństwo i zaufanie" otrzymuje brzmienie:

„Cel szczegółowy nr 3 – Cyberbezpieczeństwo i zaufanie

3.1. Liczba infrastruktur lub narzędzi z zakresu cyberbezpieczeństwa nabytych w drodze wspólnych zamówień, w tym w kontekście europejskiego systemu ostrzeżeń dotyczących cyberbezpieczeństwa

3.2. Liczba użytkowników i społeczności użytkowników uzyskujących dostęp do europejskiej infrastruktury z zakresu cyberbezpieczeństwa

3.3 Liczba działań wspierających gotowość i reagowanie na incydenty w cyberbezpieczeństwie w ramach mechanizmu cyberkryzysowego".

W odniesieniu do niniejszego aktu złożono oświadczenie, które można znaleźć w Dz.U. C, C/2025/308, 15.1.2025, ELI: http://data.europa.eu/eli/C/2025/308/oj.